Introducción a la matemática discreta

Grado en Ingeniería de Computadores

Departamento de Matemática Aplicada I.

Versión 0.3. Noviembre de 2010

Índice

I. Lógica, conjuntos, Álgebras de Boole **7**

1. Lógica . . . 9
   - 1.1. Proposiciones . . . 9
   - 1.2. Componiendo proposiciones: y, o, no, implicación, equivalencia . . . 9
   - 1.3. Equivalencia lógica de proposiciones . . . 13
   - 1.4. Cálculo de proposiciones . . . 15
2. Conjuntos . . . 18
   - 2.1. Definiciones básicas . . . 18
   - 2.2. Subconjuntos . . . 19
   - 2.3. Operaciones con conjuntos: unión, intersección, diferencia . . . 20
3. Álgebras de Boole . . . 23

II. Combinatoria **27**

1. Principios de base: principio de biyección, principio de adición, principio de producto. Recuento de palabras sin repetición. . . . 30
   - 1.1. Aplicaciones . . . 30
   - 1.2. Biyecciones . . . 32
   - 1.3. Contar sucesiones finitas . . . 34
   - 1.4. El principio de adición . . . 35
   - 1.5. El principio del producto . . . 36
2. El principio de división, el recuento de los subconjuntos de k elementos, y los números binómicos . . . 40
   - 2.1. El principio de división . . . 40
   - 2.2. Permutaciones con repeticiones . . . 42
   - 2.3. Números binómicos . . . 43
3. El principio del palomar y el principio de inclusión–exclusión . . . 47
   - 3.1. Principio de comparación . . . 47
   - 3.2. El principio del palomar . . . 49
   - 3.3. El principio de inclusión y exclusión . . . 50

III. Recursión **53**

1. Sucesiones . . . 55
   - 1.1. Introducción . . . 55
   - 1.2. Terminología . . . 55
   - 1.3. Sucesiones definidas recursivamente . . . 56
   - 1.4. Ecuaciones de recurrencia . . . 58
   - 1.5. Ecuaciones de recurrencia lineales . . . 60
2. Resolución de las ecuaciones de recurrencia lineales homogéneas a coeficientes constantes . . . 61
   - 2.1. La ecuación homogénea de orden 1 . . . 61

2.2. La ecuación homogénea de orden 2 61
2.3. La ecuación homogénea de orden cualquiera 64
3. Resolución de ecuaciones de recurrencia lineales no homogéneas a coeficientes constantes 65

LICENCIA: Esta obra está bajo una licencia "Attribution, Non–Commercial, ShareAlike" ("Reconocimiento, No commercial, Compartir Igual") 3.0 Unported de Creative Commons. Para ver una copia de esta licencia, visite:

`http://creativecommons.org/licenses/by-nc-sa/3.0/deed.es`

o envie una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

CREDITOS: Este texto está en parte derivado de los apuntes de Eric Lehman y Srinivas Devadas [1] para la asignatura *Mathematics for Computer Science* impartida en el M.I.T. Dichos apuntes estan integrados en el *MIT OpenCourseWare*.

Bibliografía

[1] Srinivas Devadas and Eric Lehman. 6.042J/18.062J Mathematics for Computer Science, Spring 2005. Massachussets Institute of Technology: MIT OpenCourseWare. `http://ocw.mit.edu` (consultado el 1ero de septiembre de 2010). Licencia: Creative Commons BY-NC-SA.

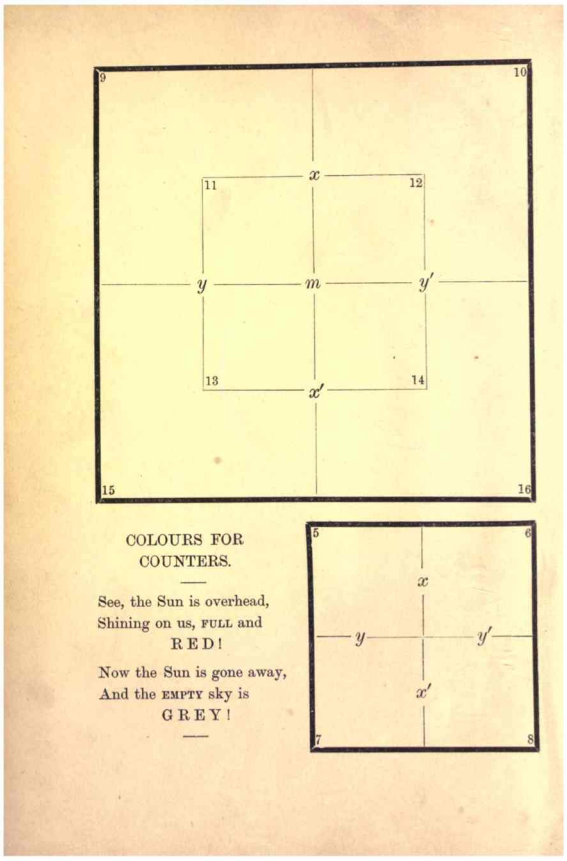
[2] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: a foundation for computer science*. Addison–Wesley, 1994.

[3] Ralph P. Grimaldi. *Matemáticas discretas y combinatoria: una introducción con aplicaciones*. Addison–Wesley Iberoamericana, 1998.

TEMA I

Lógica, Teoría de conjuntos, Álgebras de Boole

Esta parte del curso está dedicada al "lenguaje de la matemática": la lógica proposicional y la teoría de conjuntos.



1. Lógica

1.1. Proposiciones

En matemáticas, consideramos frases que son o bien verdaderas (=ciertas), o bien falsas, como las siguientes:

"$2 + 3 = 4$"
"Hoy es lunes"
"Si $x = 2$ entonces $x^2 = 4$"

Estas frases las llamamos *proposiciones*.

No son proposiciones frases como:

"Ojalá no llueva hoy !"

La frase siguiente:

"$x > 0$ y $x < 1$."

tampoco es una proposición, cuando x es una variable sin valor asignado, porque puede ser verdadera o falsa, dependiendo del valor de x. Estas frases las llamamos *predicados*.

Ejemplo 1.1 Considerese:

"Existe una infinidad de números primos p tal que $p + 2$ es primo."

No sabemos si esta frase es verdadera o falsa (es un problema sin resolver en matemáticas). Sin embargo, esta frase es bien una proposición. ◊

1.2. Componiendo proposiciones: y, o, no, implicación, equivalencia

Una proposición puede ser *compuesta*, como las siguientes:

"Hoy es lunes y llueve"
"Si llueve, no salgo"
"$5 \geq 3$ y $5 \leq 6$"

Las proposiciones que no son compuestas, las llamamos *proposiciones simples*, como:

"$5 \geq 3$".

Las proposiciones compuestas se forman a partir de proposiciones previas, por medio de las palabras: "**y**„ "**o**", "**no**", "**si** . . . **entonces** . . . ", y "**si y solo si**".

En vez de "**si** . . . **entonces** . . . " se puede decir " . . . **implica** . . . ", y en vez de "**si y solo si**" se puede decir "**es equivalente a**".

Estas palabras tienen en matemáticas un sentido muy preciso que puede diferir del sentido que se les da de manera corriente, o en otras áreas.

El conector "o"

A partir de dos proposiciones p, q se forma una nueva proposición: "p **o** q". Su valor de verdad es determinado a partir de los valores de p y de q de la manera siguiente: "p **o** q" es verdadera si por lo menos una de las dos proposiciones p, q es verdadera, y es falsa cuando ambas son falsas.

Por ejemplo,

"$5 > 3$ **o** $5 < 4$"

es verdadera, ya que "$5 > 3$" es verdadera.

Se puede resumir esta definición utilizando una "tabla de verdad":

p	q	p **o** q
V	V	V
V	F	V
F	V	V
F	F	F

Explicación: hay cuatro posibilidades para los valores de verdad de p y de q, que corresponden a las cuatro filas de la tabla. La segunda fila, por ejemplo, indica que si p es verdadera (V) y q es falsa (F) entonces "p **o** q" es verdadera (V).

Observación: Este "**o**" no es el "o exclusivo" utilizado a veces en el lenguaje corriente, como en:

"Nuestro restaurante te regala una bebida o un helado".

Este "o exclusivo" (que corresponde más explícitamente a "o bien ... o bien ...") tiene una tabla de verdad diferente de la del "**o**":

p	q	p**o**(**exclusivo**)q
V	V	F
V	F	V
F	V	V
F	F	F

El "o exclusivo" se abrevia a veces en XOR (como "e**x**clusive **or**") en ciertos lenguajes de programación. No forma parte de los conectores fundamentales de la lógica matemática.

El conector "y"

Dadas dos proposiciones p y q (por ejemplo, p es "hoy es lunes" y q es "llueve"), definimos una nueva proposición "p **y** q". Le atribuimos un valor de verdad así: "p **y** q" es verdadera si ambas proposiciones son verdaderas, y es falsa sino. O sea, es el "**y**" del lenguaje cotidiano.

La tabla de verdad de "**y**" es:

p	q	p **y** q
V	V	V
V	F	F
F	V	F
F	F	F

El conector "no"

A partir de una proposición p formamos una nueva proposición: " **no** p". La proposición " **no** p" es verdadera cuando p es falsa, y falsa cuando p es verdadera.

La tabla de verdad de la negación es:

p	**no** p
V	F
F	V

Implicación

A partir de dos proposiciones p y q formamos la nueva proposición "p **implica** q". Se puede emplear con el mismo sentido: "**si** p **entonces** q".

Con el valor de verdad de esta nueva proposición hace falta ser cauteloso. Esta definido por la tabla:

p	q	p **implica** q
V	V	V
V	F	F
F	V	V
F	F	V

En resumen:

- Para que una implicación sea verdadera, basta que la parte "si" (*hipótesis*) sea falsa, o que la parte "entonces" (*conclusión*) sea verdadera.
- La implicación es falsa si, y solo si, la hipótesis es verdadera y la conclusión es falsa.

Ejemplo 1.2

- "**si** hay vida extraterrestre **entonces** $1+1=2$"

  La implicación es correcta, aunque no sabemos si la hipótesis es cierta o no. La manera de considerar esta implicación en lógica matemática es la siguiente: la proposición no dice nada sobre lo que pasa si no hay vida extraterrestre. En particular NO dice "**si** no hay vida extraterrestre **entonces** $1+1 \neq 2$. Por lo tanto, la proposición no es falsa. Y como una proposición tiene que ser o bien cierta o bien falsa, es cierta.

- "**si** $1+1=3$ **entonces** todos los estudiantes excepto uno aprobarán la asignatura"

  La implicación es cierta, porque la hipótesis es falsa. No es necesario comprobar el valor de verdad de la conclusión.

$\Diamond$

Equivalencia

A partir de dos proposiciones p, q formamos una nueva proposición: "p **es equivalente a** q". Se puede emplear con el mismo sentido: "p **si y solo si** q" (abreviación: "p **ssi** q").

La proposición "p **es equivalente a** q" es verdadera cuando p y q tienen el mismo valor de verdad, y falsa sino:

p	q	p **es equivalente a** q
V	V	V
V	F	F
F	V	F
F	F	V

Ejemplo 1.3

- Las proposiciones siguientes son verdaderas:

  "**si** $x = 1$ **entonces** $x + 1 = 2$."
  "$x = 1$ **si y solo si** $x + 1 = 2$."

- En cambio, de las dos proposiciones siguientes:

  "**si** $x = 1$ **entonces** $x^2 = 1$."
  "$x = 1$ **si y solo si** $x^2 = -1$."

  solamente la primera es cierta. (la segunda es falsa porque para $x = -1$, se tiene que $x = 1$ es falsa pero $x^2 = 1$ es verdadera).

$\Diamond$

NOTACIONES Y TERMINOLOGÍA: En matemáticas e informática, se utilizan símbolos para representar los conectores lógicos. Están presentados en la siguiente tabla.

"p **o** q"	$p \vee q$, $p \,\|\|\, q$ (programación)
"p **y** q"	$p \wedge q$, p && q (programación)
"**no** p"	$\neg p$, $\overline{p}$, $!p$
"p **implica** q"	$p \Rightarrow q$, $p \rightarrow q$ (lógica)
"p **es equivalente a** q"	$p \Leftrightarrow q$, $p \leftrightarrow q$ (lógica)

TERMINOLOGÍA: Indicamos el sentido de unas palabras que los estudiantes encontrarán en sus lecturas. La proposición "p **y** q" es la *conjunción* de p y q, la proposición "p **o** q" es su disyunción, la proposición "**no** p" es la *negación* de p. Las palabras " **o** ", " **y** ","**no** ","**implica** ","**es equivalente a** " se llaman *conectores lógicos*.

"si" y " si y solo si " en diferentes contextos

Observación: en el lenguaje corriente se suele utilizar "si" para el " **si y solo si** " de la lógica, como en:

"**si** salgo **entonces** te llamo"

(se sobreentiende que si no salgo, no te llamo: es bien una equivalencia).

Para aumentar la confusión, en los textos de matemática las definiciones son a menudo redactas así:

"Si n es distinto de 1 y no tiene otro divisor que 1 y el mismo, decimos que n es un número primo."

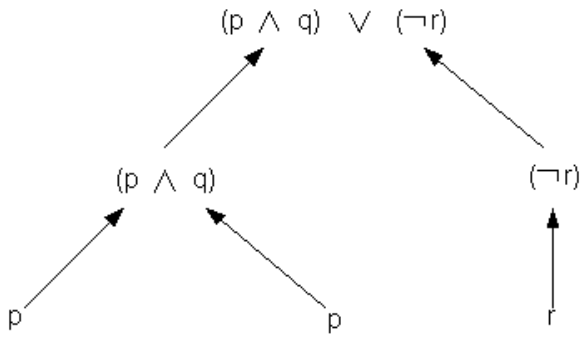
Pues hay que entenderlo como un " **si y solo si** ". En cambio, en los teoremas y en las demostraciones, los autores son más cautelosos y sus "si" son siempre los "**si**" de la lógica.

Y las paréntesis

Otro elemento que puede aparecer en una proposición son los paréntesis. Estos elementos pueden ser cruciales a la hora de expresar algo. Por ejemplo, no es lo mismo la proposición "$p \vee (q \rightarrow \neg r)$" que "$(p \vee q) \rightarrow \neg r$". La primera se leería "hoy es lunes o si el cielo está despejado entonces hoy hay luna llena", mientras que la segunda sería "si hoy es lunes o el cielo está despejado, entonces hoy hay luna llena".

Señalamos por fin que podemos representar una proposición compuesta, o una formula obtenida a partir de proposiciones indeterminadas (representadas por variables p, q ...), conectores lógicos y paréntesis, por un árbol ("árbol sinético"), en él que partiendo de las proposiciones simples, que se sitúan en la parte inferior del árbol, se van construyendo expresiones más complejas hacia arriba.

Ejemplo 1.4 Aquí está el árbol que representa la formula "$(p \wedge q) \vee (\neg r)$".



◊

1.3. Equivalencia lógica de proposiciones

Consideramos la expresión:

"p **o** ((**no** p) **y** q)"
(o sea, en símbolos: "$p \vee (\neg p \wedge q)$").

donde p y q son proposiciones sin determinar ¿ Cuales son sus posibles valores de verdad en función de los de p y de q ? Podemos contestar por un estudio exhaustivo de los casos, resumido en una tabla de verdad:

p	q	$\neg p$	$\neg p \wedge q$	$p \vee (\neg p \wedge q)$
V	V	F	F	V
V	F	F	F	V
F	V	V	V	V
F	F	V	F	F

y vemos que el valor de verdad de la expresión siempre coincide con el de "p **o** q", independientemente de los valores de verdad de p y de q. Decimos que las expresiones "(p) **o** ((**no** p) **y** q)" y "p **o** q" son *lógicamente equivalentes*.

Definición 1.1 Dos expresiones construidas a partir de variables p, q, ... (es decir letras que representan proposiciones sin determinar), conectores lógicos y paréntesis son *lógicamente equivalentes* cuando toman los mismos valores de verdad, para todos los valores de verdad posibles de p y de q.

Ejemplo 1.5 Aquí esta una aplicación del ejemplo anterior en programación. Consideramos la instrucción JAVA siguiente:

```
if (x >0 ||  (x <=0 && y > 100) )
   ...
```

(en JAVA || es el símbolo para " **o** " y && es el símbolo para " **y** "). Significa:

> Si $x > 0$ **o** ($x \leq 0$ **y** $y > 100$)
> ...

Notamos p para "$x > 0$" y q para "$y > 100$". Observamos que "$x \leq 0$" es lógicamente equivalente a **no** p. Por lo tanto, "$x > 0$ **o** ($x \leq 0$ **y** $y > 100$)" es lógicamente equivalente a "(p) **o** ((**no** p) **y** q)". Por el ejemplo anterior, es lógicamente equivalente a "p **o** q". Por lo tanto, podemos simplificar la instrucción así:

```
if (x >0 || y > 100 )
   ...
```

$\Diamond$

Una equivalencias lógicas importantes

Teorema 1.2 *"p* **si y solo si** *q" es lógicamente equivalente a "(p* **implica** *q)* **y** *(q* **implica** *p)".*

En breve: "$p \Leftrightarrow q$" es lógicamente equivalente a "$(p \Rightarrow q) \wedge (q \Rightarrow p)$".

Las demostraciones de este teorema y de los dos siguientes pueden hacerse mediante tablas de verdad.

Señalamos que la proposición $q \Rightarrow p$ se llama el *recíproco* de la implicación $p \Rightarrow q$. Una proposición y su reciproco no son lógicamente equivalentes, en general. Considerar por ejemplo:

"**si** tengo hambre **entonces** estoy de mal humor."
"**si** estoy de mal humor **entonces** tengo hambre."

Teorema 1.3 *"p* **implica** *q" es lógicamente equivalente a "(***no** *p)* **o** *q".*

En breve: "$p \Rightarrow q$" es lógicamente equivalente a $(\neg p) \vee q$.

Teorema 1.4 *"p* **implica** *q" es lógicamente equivalente a "(***no** *q)* **implica** *(***no** *p)".*

En breve: "$p \Rightarrow q$" es lógicamente equivalente a "$(\neg q) \Rightarrow (\neg p)$".

La proposición "$(\neg q) \Rightarrow (\neg p)$", lógicamente equivalente a "$p \Rightarrow q$", es llamada el *contrarrecíproco* de "$p \Rightarrow q$". Por lo tanto, cualquiera proposición es lógicamente equivalente a su contrarrecíproco.

NOTACIÓN Y TERMINOLOGÍA: Señalamos la siguiente notación por si a caso los estudiantes la encuentran: la equivalencia lógica se denota a veces con $\equiv$. Por ejemplo:

$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$$

Damos también la significación de algunas palabras importantes:

- "Contradicción": Una formula es una contradicción si es falsa para toda asignación de los valores de verdad de sus variables. Por ejemplo, "$p \Leftrightarrow \neg p$" es una contradicción: es falsa cuando p es verdadero, y falsa también cuando p es falso.
- "Tautología": Una formula es una tautología si es verdadera para toda asignación de los valores de verdad de sus variables. Por ejemplo, $(p \wedge (p \Rightarrow q)) \Rightarrow q$ es una tautología.

TERMINOLOGÍA: En los textos matemáticos se destacan ciertas proposiciones lógicas demostradas, dándoles el nombre de *Teorema*, *Proposición* (en un sentido diferente del de *proposición lógica* visto hasta ahora), de *lema* o de *corolario*. Un *teorema* es un resultado importante del texto; una *proposición* también, pero de importancia algo menor. Un *lema* es un resultado que será utilizado en la demostración de algún teorema o proposición. Un *corolario* es una consecuencia fácil de un teorema o proposición.

1.4. Cálculo de proposiciones

La expresión:

$$\neg((\neg((p \vee q) \wedge r)) \wedge (\neg q))$$

puede simplificarse en la expresión mucho más sencilla "$q \vee r$". Se puede demostrar como anteriormente utilizando tablas de verdad. Otra manera de hacer esta simplificación consiste en aplicar ciertas reglas de simplificación. Damos en el cuadro I.1 una serie de reglas de simplificación (no se pide al estudiante aprenderlas de memoria).

Veamos como simplificar la expresión "$\neg((\neg((p \vee q) \wedge r)) \vee (\neg q))$" utilizando estas reglas:

$\neg(\neg((p \vee q) \wedge r) \vee \neg q)$	**Justificación**
$= \neg(\neg((p \vee q) \wedge r)) \wedge \neg(\neg q)$	Ley de De Morgan
$= ((p \vee q) \wedge r) \wedge \neg(\neg q)$	Ley de la doble negación
$= ((p \vee q) \wedge r) \wedge q$	Ley de la doble negación
$= (p \vee q) \wedge (r \wedge q)$	Asociatividad de $\wedge$
$= (p \vee q) \wedge (q \wedge r)$	Conmutatividad de $\wedge$
$= ((p \vee q) \wedge q) \wedge r$	Asociatividad de $\wedge$
$= q \wedge r$	Ley de absorción de $\wedge$

$\overline{\overline{p}} = p$	Ley de la doble negación
$\overline{p \vee q} \Leftrightarrow \overline{p} \wedge \overline{q}$	Leyes de De Morgan
$\overline{p \wedge q} \Leftrightarrow \overline{p} \vee \overline{q}$	
$p \vee q \Leftrightarrow q \vee p$	Conmutatividad de $\vee$ y $\wedge$
$p \wedge q \Leftrightarrow q \wedge p$	
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	Asociatividad de $\vee$ y $\wedge$
$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributividad de cada una de las operaciones con respecto a la otra
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$	
$p \vee p \Leftrightarrow p$	Leyes de didempotencia
$p \wedge p \Leftrightarrow p$	
$p \vee f \Leftrightarrow p$	v y f son *neutros* para $\wedge$ y $\vee$ respectivamente.
$p \wedge v \Leftrightarrow p$	
$p \vee v \Leftrightarrow v$	Leyes de dominación
$p \wedge f \Leftrightarrow f$	
$p \vee \overline{p} \Leftrightarrow v$	$\overline{p}$ Leyes de los inversos
$p \wedge \overline{p} \Leftrightarrow f$	
$p \vee (p \wedge q) \Leftrightarrow p$	Leyes de absorción
$p \wedge (p \vee q) \Leftrightarrow p$	

Cuadro I.1: Las leyes de la lógica proposicional. Aquí v es una tautología (cualquiera), y f es una contradicciñon (cualquiera). Esta tabla esta dada a título indicativo. Si es cierto que el estudiante tiene que ser capaz de demostrar cada una de estas leyes, no se pide memorizar la lista, ni los nombres.

The chief use you will find, in such Logical skill as this Game may teach you, will be in detecting '*Fallacies*' of these two kinds.

The first kind of Fallacy——'Fallacious Premisses'——you will detect when, after marking them on the larger Diagram, you try to transfer the marks to the smaller. You will take its four compartments, one by one, and ask, for each in turn, "What mark can I place *here*?"; and in *every* one the answer will be "No information!", showing that there is *no Conclusion at all*. For instance,

"All soldiers are brave;
Some Englishmen are brave.
∴ Some Englishmen are soldiers."

looks uncommonly *like* a Syllogism, and might easily take in a less experienced Logician. But *you* are not to be caught by such a trick! You would simply set out the Premisses, and would then calmly remark "Fallacious *Premisses*!": you wouldn't condescend to ask what *Conclusion* the writer professed to draw——knowing that, *whatever* it is, it *must* be wrong. You would be just as safe as that wise mother was, who said "Mary, just go up to the nursery, and see what Baby's doing, *and tell him not to do it*!"

The other kind of Fallacy——'Fallacious Conclusion'——you will not detect till you have marked *both* Diagrams, and have read off the correct Conclusion, and have compared it with the Conclusion which the writer has drawn.

2. Conjuntos

2.1. Definiciones básicas

En matemática, un *conjunto* es una colección bien definida de objetos distintos.

Por ejemplo, podemos definir el conjunto de los números 2,4,6 y 8, e identificarlo con la letra A. En símbolos, se escribe:

$$A = \{2, 4, 6, 8\}$$

Las llaves ("{" y "}") son los símbolos reservados para la definición de un conjunto.

TERMINOLOGÍA Y NOTACIONES: Los objetos que forman un conjunto se llaman los *elementos* del conjunto. Se dice de ellos que *pertenecen al conjunto*. Que un objeto x pertenezca a (=sea elemento de) un conjunto C se nota $x \in C$, y que no pertenezca a C se nota $x \notin C$.

En el ejemplo anterior, $2 \in A$ (2 es un elemento de A, pertenece a A) pero $3 \notin A$ (3 no pertenece a A).

Hay que hacer bien la distinción entre un conjunto y sus elementos. Por ejemplo, 1 (número) es distinto de $\{1\}$ (conjunto). Especialmente, no tiene sentido "$2 \in 1$". En cambio "$2 \in \{1\}$" es una proposición bien formada (y falsa).

Otros ejemplos de conjuntos:

$\{(1,2),(3,2),(1,1)\}$	un conjunto de pares de números
$\{x, y, z\}$	un conjunto de variables
$\{\exp, \cos\}$	un conjunto de funciones
$\{\{1\},\{1,2\},\{2,5\}\}$	un conjunto de conjuntos
$\{1, \exp, \{1\}, \{1,2\}\}$	un conjunto de varios tipos de objetos.

Conjunto y orden o repetición de los elementos

La definición de un conjunto no toma en cuenta ningún orden de sus elementos. El conjunto A del ejemplo anterior pude igualmente definirse como $\{2, 6, 4, 8\}$, o $\{8, 6, 4, 2\}$, o ... Las collecciones ordenadas de objetos se llaman *sucesiones* y se suelen notar con paréntesis, como por ejemplo $(2, 4, 6, 8)$ (una sucesión con cuatro términos), o $(2, 6, 4, 8)$ (una sucesión distinta de la anterior).

Observar que, por definición, un conjunto tiene sus elementos distintos, por lo cual es incorrecto escribir $\{2, 4, 2\}$. En cambio, una sucesión puede tener elementos repetidos: $(2, 4, 2)$ es una sucesión bien definida.

Conjuntos finitos y conjuntos infinitos

Un conjunto puede ser *finito* o *infinito*. El número de elementos de un conjunto finito se llama su *cardinal*, y se nota con doble barra $|\ \ |$ o con $\#$. Por ejemplo, si $A = \{2, 4, 6, 8\}$ entonces $|A| = 4$ ("A tiene cuatro elementos" o "A tiene cardinal cuatro") . Se puede notar también $\#A = 4$.

Ciertos conjuntos infinitos importantes se identifican con símbolos reservados:

símbolo	conjunto	elementos
$\mathbb{N}$	enteros naturales	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	enteros	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Q}$	números racionales	$\frac{1}{2}, -\frac{10}{3}, 1\ldots$
$\mathbb{R}$	números reales	$\sqrt{2}, \pi, \frac{1}{2}, 1\ldots$
$\mathbb{C}$	números complejos	$i, \frac{1+i}{2}, \sqrt{2}, \frac{1}{2}, 1, \ldots$

Definir un conjunto por una propiedad característica de sus elementos

En vez de definir un conjunto dando la lista explicita de sus elementos, se puede definir dando una propiedad característica de sus elementos. Por ejemplo:

> Sea B el conjunto de todos los números enteros pares n que cumplen $n \geq 2$ y $n < 9$.

Esta definición se escribe con símbolos de la manera siguiente:

$$B = \{n \mid \ n \text{ es un entero y } n \geq 2 \text{ y } n < 9\}$$

Explicación:

- Las llaves "{" y "}" indican que se va a definir un conjunto.
- "$\{n \mid \ldots\}$" se lee "el conjunto de los n tal que ..." y a continuación se da la propiedad característica de los elementos del conjunto.

Mencionar que la letra n no juega ningún papel particular, y se puede igualmente definir B como, por ejemplo:

$$B = \{w \mid \ w \text{ es un entero y } w \geq 2 \text{ y } w < 9\}$$

El conjunto vacío

El conjunto más pequeño de todos es $\{\ \ \}$, el *conjunto vacío*. Es el conjunto sin ningún elemento. Se suele notar con $\emptyset$. Su cardinal es 0. Tiene muchas descripciones: para una propiedadad dada que nunca se da, es el conjunto de los elementos que cumplen esta propiedad. Por ejemplo:

$$\emptyset = \{x \mid x \in \mathbb{N} \text{ y } x + 1 = x\}, \qquad \emptyset = \{x \mid 0 = 1\}.$$

2.2. Subconjuntos

Dados dos conjuntos A y B, se dice que A es un *subconjunto* de B si todo elemento de A es también elemento de B. Se nota $A \subset B$ cuando A es un subconjunto de B (la notación debe evocar "A es más pequeño que B"), y $A \not\subset B$ cuando no lo es.

Ejemplos:

- $\{1, 2\} \subset \{1, 2, 3\}$ pero $\{1, 4\} \not\subset \{1, 2, 3\}$ ya que $4 \notin \{1, 2, 3\}$.
- $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

- $\emptyset \subset \{1,2\}$. De hecho, $\emptyset$ es un subconjunto de todos los conjuntos.
- Los subconjuntos de $\{1,2\}$ son: $\emptyset$, $\{1\}$, $\{2\}$ y $\{1,2\}$.

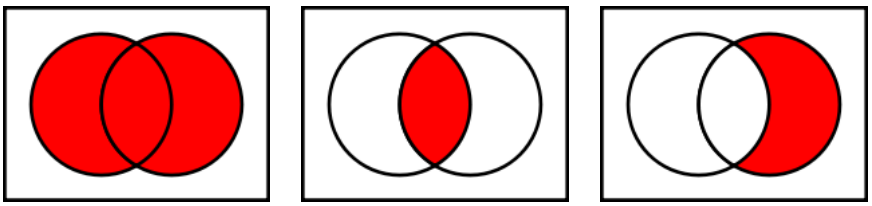
TERMINOLOGÍA: Para decir que A es un subconjunto de B, se dice también que A es *una parte* de B, que A *esta contenido en* B, que A esta incluido en B, o que B *contiene* A.

2.3. Operaciones con conjuntos: unión, intersección, diferencia

Consideramos como ejemplo para las definiciones que siguen $X = \{1,2,3\}$ e $Y = \{1,3,5,7\}$.

- La *unión* $A \cup B$ de dos conjuntos A y B es el conjunto de los objetos que pertenecen a (por lo menos) uno de los dos conjuntos. Ejemplo: $X \cup Y = \{1,2,3,5,7\}$.
- La *intersección* $A \cap B$ de dos conjuntos A y B es el conjunto de los objetos que pertenecen a sendos conjuntos A e B. Ejemplo: $X \cap Y = \{1,3\}$.
- La *diferencia* $A \setminus B$ ("A menos B") es el conjunto de los objetos que pertenecen a A pero no a B. Ejemplo: $X \setminus Y = \{2\}$, $Y \setminus X = \{5,7\}$. Se nota también a veces $A - B$

Representamos convenientemente los subconjuntos $A \cup B$, $A \cap B$, $B \setminus A$ mediante diagramas como los siguientes (los dos discos representan A y B).



TERMINOLOGÍA: Cuando B es un subconjunto de A, entonces la diferencia $A \setminus B$ se llama también *complementario de* A *en* B. A menudo, el conjunto A es fijado sin ambigüedad. En este caso el complementario de B en A se nota $\overline{B}$.

MÁS TERMINOLOGÍA: Se dice de dos conjuntos A y B son *disjuntos* si su intersección es vacía ($A \cap B = \emptyset$).

Es interesante observar que la unión y la intersección son operaciones sobre conjuntos, como la adición es una operación sobre números.

Ejemplo 2.1 Podemos construir las tablas de unión y de intersección para los subconjuntos de $\{1,2\}$:

$\cup$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\{1\}$	$\{1,2\}$	$\{1,2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\{2\}$	$\{1,2\}$
$\{1,2\}$	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$	$\{1,2\}$

$\cap$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$	$\{1\}$
$\{2\}$	$\emptyset$	$\emptyset$	$\{2\}$	$\{2\}$
$\{1,2\}$	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$

$\Diamond$

$\overline{\overline{A}} = A$	Ley del doble complemento
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	Leyes de De Morgan
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Conmutatividad de $\cup$ y $\cap$
$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	Asociatividad de $\cup$ y $\cap$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributividad de cada una de las operaciones con respecto a la otra
$A \cup A = A$ $A \cap A = A$	A es idempotente para ambas operaciones
$A \cup \emptyset = A$ $A \cap X = A$	X y $\emptyset$ son *neutros* para $\cap$ y $\cup$ respectivamente.
$A \cup X = A$ $A \cap \emptyset = \emptyset$	X y $\emptyset$ son *absorbentes* para $\cup$ y $\cap$ respectivamente.
$A \cup \overline{A} = X$ $A \cap \overline{A} = \emptyset$	$\overline{A}$ es inversa de A para $\cup$ y $\cap$
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Leyes de absorción

Cuadro I.2: Las leyes de la teoría de conjuntos

Sabemos que la adición y las multiplicación de los números son "conmutativas" ($a + b = b + a$, $a \times b = b \times a$), "asociativas" ($(a + b) + c = (a + (b + c))$ y similarmente para $\times$, pero al contrario de la división, por ejemplo), que la multiplicación es distributiva con respecto a la adición ($a \times (b + c) = (a \times b) + (a \times c)$). Podemos, de manera similar, hacer una lista de propiedades de las operaciones $\cup$, $\cap$ y complementario sobre los subconjuntos de un conjunto fijo X: ver el cuadro I.2

Todas estas reglas pueden ser utilizadas en un "cálculo de conjuntos", por ejemplo para simplificar formulas.

Ejemplo 2.2 Consideramos un conjunto X y los subconjuntos A, B y C de X. Vamos a simplificar la expresión $\overline{\overline{(A \cup B) \cap C} \cup \overline{B}}$, utilizando las reglas del cuadro I.2.

$\overline{\overline{(A \cup B) \cap C} \cup \overline{B}}$	**Justificación**
$= \overline{\overline{(A \cup B) \cap C}} \cap \overline{\overline{B}}$	Ley de De Morgan
$= ((A \cup B) \cap C) \cap \overline{\overline{B}}$	Ley del doble complemento
$= ((A \cup B) \cap C) \cap B$	Ley del doble complemento
$= (A \cup B) \cap (C \cap B)$	Asociatividad de $\cap$
$= (A \cup B) \cap (B \cap C)$	Conmutatividad de $\cap$
$= ((A \cup B) \cap B) \cap C$	Asociatividad de $\cap$
$= B \cap C$	Ley de absorción de $\cap$

$\Diamond$

Finalmente, vamos a dar una demostración de unas de estas reglas, dejando la demostración de las otras como ejercicio.

Demostramos que para cualquieres subconjuntos A y B de un conjunto X, se tiene $\overline{A \cup B} = \overline{A} \cap \overline{B}$ (una de las leyes de De Morgan).

Demostración. Sea $x \in X$. Por definición del complementario, "$x \in \overline{A \cup B}$" es equivalente a "$x \notin A \cup B$". Es la negación de: "$x$ pertenece a A o a B". Por lo tanto, es equivalente a "x no pertenece ni a A ni a B", que es equivalente a "$x \in \overline{A} \cap \overline{B}$". Esto establece que $x \in \overline{A \cup B}$ si y solo si $x \in \overline{A} \cap \overline{B}$. Los dos conjuntos tienen los mismos elementos, por lo tanto son iguales. □

Demostramos que para cualquieres conjuntos A, B y C, se tiene $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributividad de $\cap$ con respecto a $\cup$).

Demostración. Vamos a demostrar en primero que $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$, y luego que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. O sea: que todo elemento del primer conjunto es elemento del segunda, y *vice–versa*. Esto demostrará bien que los dos conjuntos tienen los mismos elementos, o sea: que son iguales. (Este tipo de demostración de la igualdad de dos conjuntos de llama "demostración de la doble–inclusión").

Demostremos $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Sea $x \in A \cap (B \cup C)$. En particular $x \in A$, y $x \in B \cup C$. Por lo tanto $x \in B$ o $x \in C$. En el primer caso ($x \in B$), obtenemos $x \in A \cap B$. En el segundo caso ($x \in C$), obtenemos $x \in A \cap C$. En ambos casos podemos concluir que $x \in (A \cap B) \cup (A \cap C)$. Esta así demostrada la inclusión anunciada. En efecto, hemos comprobado que todo elemento x de $A \cap (B \cup C)$ pertenece también a $(A \cap B) \cup (A \cap C)$.

Demostremos ahora que $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Sea $x \in (A \cap B) \cup (A \cap C)$. Otra vez examinamos los dos casos posibles: $x \in (A \cap B)$ o $x \in (A \cap C)$. En el primer caso tenemos $x \in A$. Tenemos también $x \in B$ y por lo tanto $x \in (B \cup C)$. Concluimos que $x \in A \cap (B \cup C)$. El segundo caso se trata de la misma manera, intercambiando los papeles de B y C. En ambos casos, $x \in A \cap (B \cup C)$. esto demuestra la inclusión anunciada, y acaba la demostración de la igualdad de los conjuntos. □

3. Álgebras de Boole

El álgebra de conjuntos y el álgebra de proposiciones presentan grandes paralelismos. Hay un concepto matemático que generaliza ambas teorías, y otras: el concepto de *álgebra de Boole*.

Definición 3.1 Un álgebra de Boole es un conjunto B con dos operaciones, que se suelen llamar *suma* y *producto* y notar con $+$ y $\times$ (o, a veces, por solamente un punto: $\cdot$), y una transformación que asocia a cada elemento de x un elemento x' de B que se suele llamar complementario, tal que los axiomas siguientes se verifican:

Axioma 1. Las operaciones $(+)$ y $(\times)$ son conmutativas:

a) $x + y = y + x$

b) $x \times y = y \times x$

Axioma 2. Las operaciones $(+)$ y $(\times)$ son asociativas:

a) $(x + y) + z = x + (y + z)$

b) $(x \times y) \times z = x \times (y \times z)$

Axioma 3. Las operaciones $(+)$ y $(\times)$ son distributivas, cada una sobre la otra:

a) $x + (y \times z) = (x + y) \times (x + z)$

b) $x \times (y + z) = x \times y + (x \times z)$

Axioma 4. Existen elementos de B, notados 0 y 1, *neutros* para $(+)$ y $(\times)$ respectivamente. Significa:

a) $x + 0 = x$ para todo $x \in B$.

b) $x \times 1 = x$ para todo $x \in B$.

Axioma 5. Para todo elemento x de B, se cumple:

a) $x + x' = 1$

b) $x \times x' = 0$

Ejemplos fundamentales:

- Sea X un conjunto. Entonces el conjunto de todos los subconjuntos de X, con $\cup$ y $\cap$ para las operaciones $+$ y $\times$, y $A' = \overline{A}$ para el complementario, es un álgebra de Boole.
- El conjunto $\{V, F\}$ (conjunto de los dos valores de verdad) es un álgebra de Boole, con $\wedge$ y $\vee$ como operaciones $+$ y $\times$, y $p' = \neg p$ para el complementario, es un álgebra de Boole.

Para demostrar que estas álgebras son efectivamente álgebras de Boole habría que probar que verifican los cinco axiomas que definen un álgebra de Boole.

Sin sorpresa, la lista de propiedades que hemos enunciado para subconjuntos de un conjunto y para proposiciones vale en toda generalidad para las álgebras de Boole:

$(x')' = x$	Ley del doble complementario
$(x+y)' = x' \times y'$	Leyes de De Morgan
$(x \times y)' = x' + y'$	
$x + y = y + x$	conmutatividad de + y $\times$
$x \times y = y \times x$	
$(x+y)+z = x+(y+z)$	asociatividad de + y $\times$
$(x \times y) \times z = x \times (y \times z)$	
$x \times (y+z) = (x \times y) + (x \times z)$	Distributividad de cada una de las operaciones con respecto a la otra
$x + (y \times z) = (x+y) \times (x+z)$	
$x + x = x$	cada x es idempotente para ambas operaciones
$x \times x = x$	
$x + 0 = x$	1 y 0 son *neutros* para $\times$ y + respectivamente.
$x \times 1 = x$	
$x + 1 = x$	Leyes de dominación
$x \times 0 = 0$	
$x + x' = 1$	Leyes de los inversos
$x \times x' = 0$	
$x + (x \times y) = x$	Leyes de absorción
$x \times (x+y) = x$	

Cuadro I.3: Las leyes de las álgebra de yoole

Como ilustración, enseñamos la demostración abstracta de la ley de dominación $x+1 = x$ directamente a partir de los aximas:

$x+1$	$= 1 \cdot (x+1)$	por Axioma $4b$
	$= (x+x') \cdot (x+1)$	por Axioma $5a$
	$= x + (x' \times 1)$	por Axioma $3a$
	$= x + x'$	por Axioma $4b$
	$= 1$	por Axioma $5a$.

Otro ejemplo: circuitos de conmutación

En otra asignatura los estudiantes encontrarán un ejemplo más de álgebras de Boole: la *álgebra de conmutación* del análisis de circuitos electrónicos. Se consideran *circuitos de conmutación* como él de la figura I.1. Un circuito de conmutación consiste en un *conjunto*

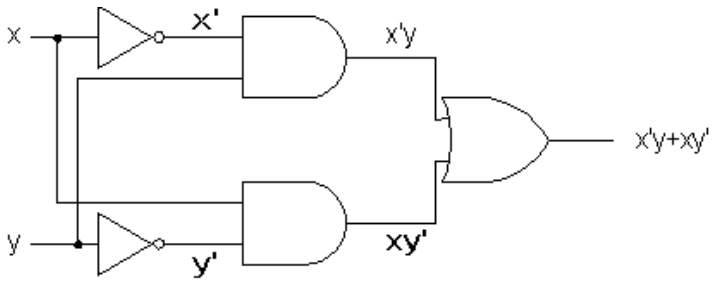
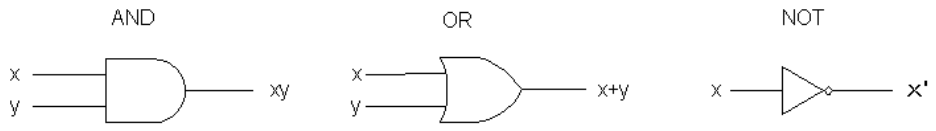


Figura I.1:

de entradas, un *procesador* y un *conjunto de salidas*. Las entradas y las salidas se suelen representar gráficamente como segmentos. Son variables que toman los posibles valores binarios, en función de si están activas o no: cuando circula corriente a través de ellas toman el valor 1; en caso contrario toman el valor 0. Esto hace que los circuitos sean considerados sistemas binarios. El procesador se compone de distintos componentes simples que se pueden combinar entre sí y a los que se denomina *puertas*. Fundamentalmente se utilizan tres puertas: *AND*, *OR*, *NOT*. Gráficamente se representan mediante distintos símbolos, aunque quizá los más usuales son:



El *álgebra de conmutación* es el álgebra de Boole cuyo conjunto es $\{0,1\}$ y cuyas operaciones $+$, $\times$ y complementario son definidas por las tablas:

$+$	0	1
0	0	1
1	1	1

$\times$	0	1
0	0	0
1	0	1

x	x'
0	1
1	0

Es fácil comprobar que se trata de una reescritura de álgebra de Booles de la lógica proposicional, tomando $F = 0$, $V = 1$, $+ = \vee$, $\times = \wedge$, $' = \neg$.

Las operaciones son realizadas por las puertas:

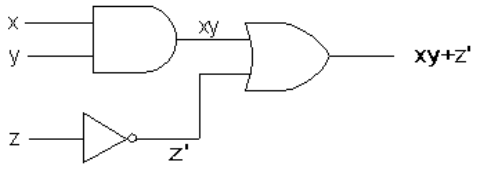
- La puerta AND actúa sobre dos variables binarias x, y mediante la operación $\times$, de manera que las entradas son las dos variables x, y y la salida es xy.

- La puerta OR actúa sobre dos variables binarias x, y mediante la operación $+$, siendo las entradas las dos variables x, y y la salida el valor correspondiente a $x + y$.

- La puerta NOT actúa sobre una variable x mediante la operación $'$, de forma que la entrada es la variable x y la salida es x'.

Ejemplo 3.1 El circuito de la figura I.1 representa la función de conmutación $x'y + xy'$. $\Diamond$

Ejemplo 3.2 Veamos qué circuito produce la función de conmutación $xy + z'$:



NOTA BENE.

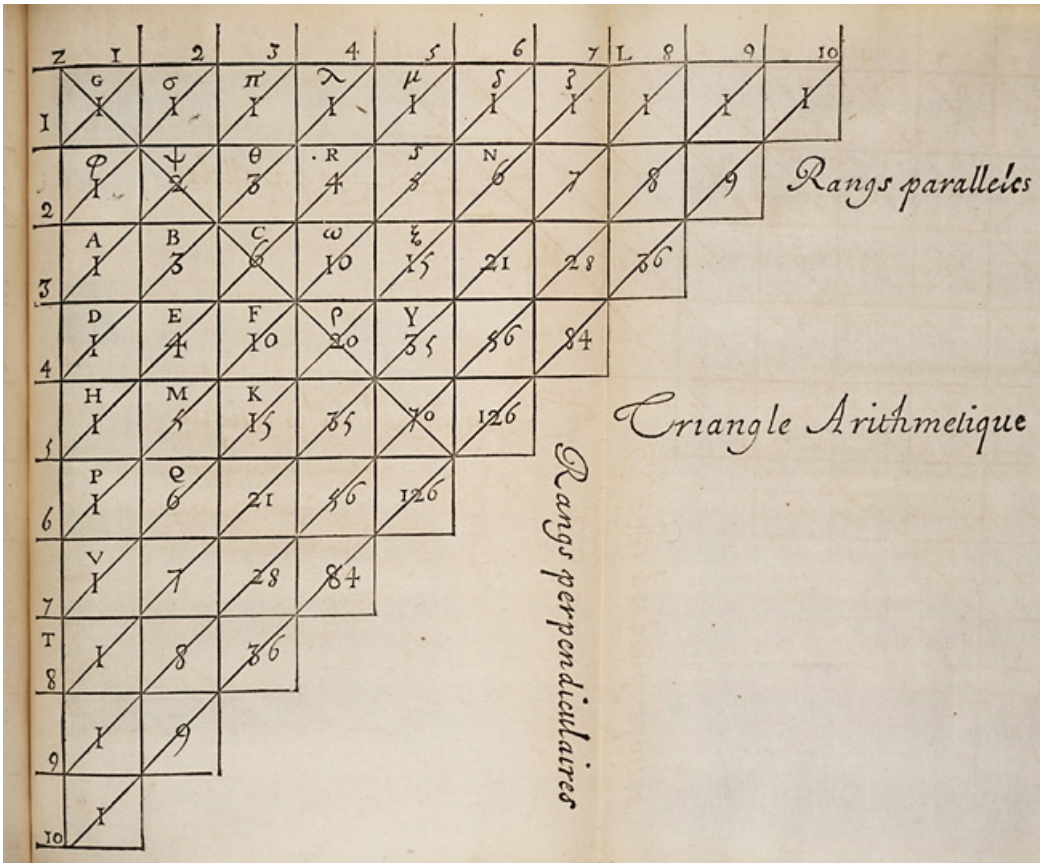
With each copy of this Book is given an Envelope, containing a Diagram (similar to the frontispiece) on card, and nine Counters, four red and five grey.

The Envelope, &c. can be had separately, at 3*d.* each.

The Author will be very grateful for suggestions, especially from beginners in Logic, of any alterations, or further explanations, that may seem desirable. Letters should be addressed to him at "29, Bedford Street, Covent Garden, London."

TEMA II

Combinatoria



Introducción

En esta parte del curso presentamos una variedad de reglas y principios para contar: dado un conjunto finito, ¿ Podemos contar sus elementos (sin hacer la lista de dichos elementos, claro está) ?

Ejemplo 0.3 **Pregunta:** Si cinco niños comparten 12 canicas idénticas ¿ De cuantas maneras pueden repartírselas ?

(Por ejemplo: 2 para el primer niño, 2 para el segundo, ninguna para el tercero, 5 para el cuarto y 3 para el último)

Pregunta: ¿ Cuántos números de 16 bits tienen *exactamente* cuatro "1" ?

(Por ejemplo 0010011000001000.)

Sorprendentemente, las dos preguntas tienen la misma respuesta. Vamos a ver el *porque*. De momento sólo daremos una indicación:

$$\cdot\cdot\,|\,\cdot\cdot|\,|\,\cdot\cdot\cdot\cdot\cdot\,|\,\cdot\cdot$$

$\Diamond$

¿ Qué vamos a contar ?

¿ Puede ya contestar a algunas de estas preguntas ?

- Todos los subconjuntos de un conjunto de 10 elementos (como por ejemplo: $\emptyset$, $\{1\}$, $\{1,2\}$, $\{2\}$ ... para el conjunto $\{1,2,3,\ldots,10\}$).
- Los subconjuntos de 4 elementos de un conjunto de 16 elementos (como por ejemplo $\{3,6,7,13\}$ para el conjunto $\{1,2,3,\ldots,16\}$).
- Las soluciones enteras positivas o nulas de la ecuación $x_1+x_2+x_3+x_4+x_5=12$. (Por ejemplo $x_1=2$, $x_2=2$, $x_3=0$, $x_4=5$, $x_5=3$.)
- Los números de 16 bits, exactamente cuatro de ellos siendo "1" (como por ejemplo 0010011000001000).
- Los anagramas de la palabra CONTAR (son CORNAT, RNTCAO, ...)
- Los anagramas de la palabra CASCARA (son AAARCCS, CARACAS, ...).

¿ Piensa que en Sevilla (capital) hay por lo menos cuatro personas que tienen el mismo número de cabellos ?

¿ Por qué contar ?

Contar es útil en informática por varias razones. Entre otras:

- Determinar el tiempo y la memoria necesarios para la resolución de un problema de cálculo se reduce a menudo a un problema de contar.
- Contar es la base de las probabilidades.

1. Principios de base: principio de biyección, principio de adición, principio de producto. Recuento de palabras sin repetición.

En esta lección presentamos tres principios básicos de contar. Aunque son muy simples, ya permiten resolver una gran cantidad de problemas.

1.1. Aplicaciones

Damos en primer lugar una definición simple, pero algo incorrecta, de *aplicación* : una *aplicación* (o *función*) de un conjunto A en un conjunto B es una regla para asociar a cada elemento de A un elemento de B.

Ejemplo 1.1 Con $A = B = \mathbb{Z}$ definimos la función f siguiente de A en B:

$$f(n) = \begin{cases} n/2 \text{ si } n \text{ es par} \\ (n-1)/2 \text{ si } n \text{ es impar} \end{cases}$$

Pero podríamos definir igualmente f de la manera siguiente: $f(n)$ es el mayor entero k de los que cumplen $2\,k \leq n$. ◊

Este ejemplo nos hace ver una limitación de la definición anterior: una aplicación *no es* una regla, ya que una aplicación dada puede ser definida por *varias* reglas. Esto nos conduce a una definición más abstracta, pero más general, de aplicación: consiste en decir que una aplicación f es un conjunto de pares ordenados, el conjunto de todos los $(a, f(a))$ donde a es elemento de A. Es lo que vamos a formalizar a continuación.

Ejemplo 1.2 Quizás estamos acostumbrados a pensar que el conjunto de puntos (x, x^2) para $x \in \mathbb{R}$ (una parábola) es solamente un objeto asociado a la aplicación $x \mapsto x^2$ de $\mathbb{R}$ en $\mathbb{R}$ (su *gráfica*). Con la definición abstracta, consideraremos que dicha gráfica *es* la aplicación. ◊

Necesitamos unas definiciones preliminares.

Definición 1.1 Dados dos conjuntos A y B, el conjunto de todos los pares ordenados (a, b) donde a está en A y b en B se denomina *producto cartesiano* de A por B, y se nota $A \times B$.

Ejemplo 1.3 Si $A = \{1, 2, 3\}$ y $B = \{a, e\}$, entonces el producto cartesiano $A \times B = \{(1, a), (1, e), (2, a), (2, e), (3, a), (3, e)\}$. Podemos representarlo mediante una tabla:

	1	2	3
a	(1,a)	(2,a)	(3,a)
e	(1,e)	(2,e)	(3,e)

Esto nos deja ver claramente que, si los conjuntos A y B son finitos, entonces $|A \times B| = |A| \cdot |B|$ (el cardinal del producto cartesiano es el producto de los cardinales). ◊

Ejemplo 1.4 El conjunto $\mathbb{R} \times \mathbb{R}$ (también notado $\mathbb{R}^2$) es el conjunto de todos los pares ordenados de números reales: los (x, y), que podemos identificar a los puntos del plano. $\Diamond$

Definición 1.2 Una *correspondencia* entre los conjuntos A y B es cualquier subconjunto del producto cartesiano $A \times B$. Si un par (a, b) pertenece a una correspondencia, diremos que al elemento origen a le corresponde el elemento destino b.

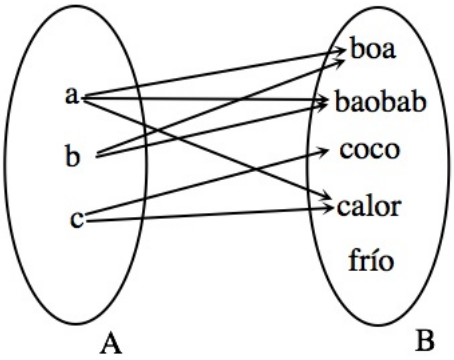
Ejemplo 1.5 Consideramos para A el conjunto de letras $\{a, b, c\}$ para B el conjunto de palabras $\{\text{boa}, \text{baobab}, \text{coco}, \text{calor}, \text{frío}\}$. Definimos la correspondencia C "es letra de" entre A y B. *Formalmente* , es el conjunto siguiente:

$$C = \{(a, boa), (a, baobab), (a, calor), (b, boa), (b, baobab), (c, coco), (c, calor)\}$$

aunque en general no nos conviene pensarlo así. Preferimos presentarlo por medio de una tabla :

C	boa	baobab	coco	calor	frío
a	×	×		×	
b	×	×			
c			×	×	

o de un diagrama, trazando una flecha desde x hasta y cada vez que al elemento origen x le corresponde el elemento destino y:



$\Diamond$

Definición 1.3 Una *aplicación* de A en B es una correspondencia tal que a cada elemento de A le corresponde uno y sólo un elemento de B.

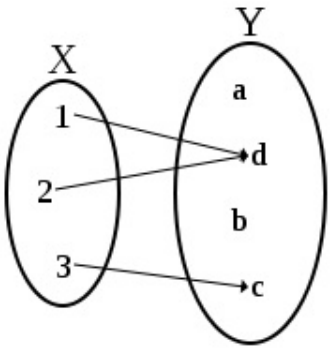
TERMINOLOGÍA: Si f es una aplicación de A en B entonces:

- A se llama el *conjunto de partida* de f (también su *dominio*).
- B se llama el *conjunto de llegada* de f.
- Para $a \in A$, el único elemento b de B que le corresponde por f se llama *imagen de a por f*. Se nota $b = f(a)$.

- Para $b \in B$, los elementos $a \in A$ que le corresponden por f (es decir: tal que $f(a) = b$) se llaman los *antecedentes de b*.

Ejemplo 1.6

- La correspondencia del ejemplo 1.5 no es una aplicación, ya que, por ejemplo, al elemento a del conjunto origen A corresponden varios elementos de B.
- El diagrama siguiente representa bien una aplicación:



$\Diamond$

NOTACIÓN: La notación $f : A \to B$ significa: "f es una aplicación de A en B". Si f es definida por una regla se puede notar:

$$\begin{array}{rccc} f: & A & \to & B \\ & a & \mapsto & \text{descripción de la regla} \end{array}$$

Por ejemplo para definir la función f de los enteros en los enteros que cumple $f(n) = \frac{n(n+1)}{2}$ se puede notar:

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & \frac{n(n+1)}{2} \end{array}$$

1.2. Biyecciones

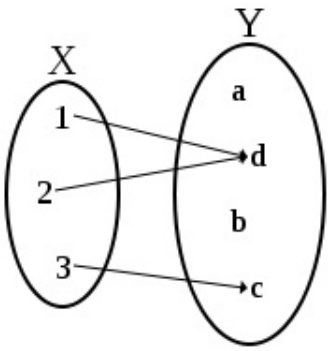
Observar que la definición de una aplicación de A en B es algo asimétrica: a cada elemento de A debe corresponder uno y sólo un elemento de B, mientras que a un elemento de B le puede corresponder uno, varios o ningún elemento de A.

Las *biyecciones* son las aplicaciones para las cuales la simetría se restablece.

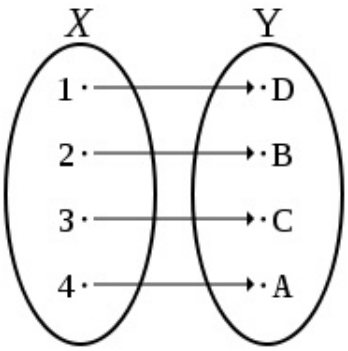
Definición 1.4 Sea f una aplicación de A en B. Es una *biyección* cuando todo elemento de B es imagen de uno, y sólo un elemento de A.

Ejemplo 1.7

- Contar los elementos de un conjunto finito es establecer una biyección del conjunto de un conjunto de la forma $\{1, 2, 3, \ldots, n\}$.
- Las herramientas de medida físicas utilizan biyecciones entre magnitudes físicas (por ejemplo entre temperatura y altura de una columna de alcohol para un termómetro).
- La aplicación de $X = \{1, 2, 3\}$ en $Y = \{a, b, c, d\}$ representada por el diagrama siguiente no es una biyección. En efecto, hay elementos sin antecedentes (como b por ejemplo). También hay un elemento con más de un antecedente (el elemento d).



- En cambio la aplicación de $X = \{1, 2, 3, 4\}$ en $Y = \{A, B, C, D\}$ representada por el diagrama siguiente es una biyección.



◊

Regla 1 *(Regla de la biyección) Sean A y B dos conjuntos finitos. Si existe una biyección de A en B entonces A y B tienen mismo cardinal.*

Ejemplo 1.8 continuación del ejemplo 0.3 Conisideramos otra vez los dos problemas:

- Contar las maneras de repartir 12 canicas idénticas entre 5 niños.
- Contar los números de 16 bits con exactemente cuatro "1".

Sea A el conjunto de todas las maneras posibles de repartir las 12 canicas entre los 5 niños. Una repartición esta caracterizada por los números de canicas x_1, x_2, x_3, x_4, x_5 recibidas por cada niño.

Sea B el conjunto de los números de 16 bits con exactamente cuatro "1".

Definimos una aplicación $f : A \to B$ de la manera siguiente: $f(x_1, x_2, x_3, x_4, x_5)$ es el número que se escribe:

$$\overbrace{00\cdots0}^{x_1}1\overbrace{00\cdots0}^{x_2}1\overbrace{00\cdots0}^{x_3}1\overbrace{00\cdots0}^{x_4}1\overbrace{00\cdots0}^{x_5}$$

Por ejemplo: $f(2, 2, 0, 5, 3) = 0010011000001000$.

Vemos que todo número de 16 bits con cuatro 1 es imagen de uno, y sólo un elemento $(x_1, x_2, x_3, x_4, x_5)$ de A: x_1 es el número de ceros que preceden el primer "1", x_2 es el número de ceros entre el primero y el segundo "1", ... Por lo tanto f es una biyección de A en B. Por el principio de la biyección, A y B tienen el mismo número de elementos. $\Diamond$

1.3. Contar sucesiones finitas

La estrategia para contar presentada en este curso es la siguiente:

1. Vamos a desarrollar técnicas para contar un tipo muy especial de objetos matemáticos: las sucesiones finitas.
2. Cada vez que encontremos un problema de recuento, reduciremos el problema a un recuento de sucesiones. Más precisamente, buscaremos una biyección entre el conjunto a contar y un conjunto de sucesiones.

Llamamos *sucesiones* a las colecciones ordenadas de objetos como las siguientes:

- $(0, 0, 1, 0, 1, 1, 0)$, un ejemplo de sucesión de bits.
- $(12, 15, -3, 5, 7)$, un ejemplo de sucesión de números.
- (C, A, S, C, A, R, A) y (R, O, M, A) son ejemplos de sucesiones de caracteres.

El orden importa: la sucesión (R, O, M, A) es distinta de (A, M, O, R). Por esto marcamos la sucesión con paréntesis "$(\ldots)$" en vez de llaves "$\{\ldots\}$". También una sucesión no tiene por que tener términos distintos.

Los ejemplos anteriores son ejemplos de sucesiones finitas. Las sucesiones infinitas existen también, pero no las encontraremos en el estudio de este tema.

TERMINOLOGÍA: Los objetos que aparecen en una sucesión se llaman sus *términos*. Son numerados a partir de 1: el primer elemento de (C, A, S, C, A, R, A) es "C", el segundo es "A", el tercero es "S", el cuarto es "C" también ... El número de términos de una sucesión finita se llama su *longitud*. La sucesión (C, A, S, C, A, R, A) tiene longitud 7, aunque la sucesión tiene solamente 4 términos distintos.

Observar que las sucesiones de longitud 2 son los *pares ordenados* mencionados en la definición 1.5. Extendemos esta definición a más de dos conjuntos:

Definición 1.5 Dados los conjuntos A_1, A_2, ..., A_n, entonces el conjunto de todas las sucesiones de longitud n cuyo primer termino pertenece a A_1, segundo termino a A_2, ..., n–esimo termino a A_n se llama *producto cartesiano de los conjuntos* A_1, A_2, ..., A_n. Se nota $A_1 \times A_2 \times \cdots \times A_n$.

NOTACIÓN: El producto cartesiano de n veces el mismo conjunto A se puede notar A^n en vez de $A \times A \times \cdots A$.

Las sucesiones cuyos términos pertenecen todos a un mismo conjunto A se presentan de otras dos maneras: como *palabras* y como *aplicaciones*. Nos da tres presentaciones diferentes de los mismos objetos, cada una con una terminología propia.

Terminología:	**Ejemplo y notaciones correspondentes** con $A = \{a, c, r, s, t\}$ y $n = 7$
"Sucesiones de longitud n con términos en A"	(c,a,s,c,a,r,a)
"Palabras de longitud n en el alfabeto A"	cascara
"Aplicaciones de $\{1, 2, \ldots, n\}$ en A"	La función f de $\{1, 2, 3, 4, 5, 6, 7\}$ en A con $f(1) = c$, $f(2) = a$, $f(3) = s$, $f(4) = c$, $f(5) = a$, $f(6) = r$ y $f(7) = a$.

1.4. El principio de adición

Ejemplo 1.9 Si sabemos que en una clase hay 6 personas de no más de 18 años (conjunto A de personas), y 7 personas de entre 19 y 22 años (conjunto B), entonces podemos concluir que son 13 personas de no más de 22 años:

$$|A \cup B| = |A| + |B|$$

En cambio, si sólo sabemos que hay 6 personas de no más de 18 años (conjunto A), y 7 personas de entre 17 y 22 años (conjunto B), no somos capaces de dar el número exacto de personas de no más de 22 años. En particular, en este caso, $|A \cup B|$ puede ser diferente de $|A| + |B|$. ◊

Este ejemplo ilustra el caso más simple del *principio de adición*: si dos conjuntos A y B son disjuntos (es decir su intersección es vacía), se verifica que

$$|A \cup B| = |A| + |B|$$

Presentamos ahora la forma más general de este principio. Decimos de conjuntos A_1, A_2, ..., A_n que son *disjuntos dos a dos* si cada par de estos conjuntos tiene intersección vacía: $A_1 \cap A_2 = \emptyset$, $A_1 \cap A_3 = \emptyset$, $A_2 \cap A_3 = \emptyset$, ...

Regla 2 *(Principio de adición) Si los conjuntos* A_1, A_2, ..., A_n *son disjuntos dos a dos, entonces*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

1.5. El principio del producto

El principio

Ejemplo 1.10 ¿ Cuántas palabras de longitud 4 podemos formar con las letras a, c, s ?

Solución: Tenemos 3 posibilidades para cada una de las letras. Obtenemos $3\times3\times3\times3 = 3^4 = 81$ palabras posibles. ◊

Ejemplo 1.11 En una promoción de 50 estudiantes, se reparten un primer premio, un segundo premio y un tercer premio. ¿ Cuales son las reparticiones posibles ?

Solución: Hay 50 posibilidades para atribuir el primer premio. Para atribuir el segundo premio solamente hay 49 posibilidades, ya que hay que excluir el laureado del primer premio. Y para atribuir el tercer premio quedan solamente 48 posibilidades. Hay por lo tanto $50 \times 49 \times 48$ reparticiones posibles. ◊

Regla 3 (Principio del producto) *Sea S un conjunto de sucesiones de longitud n tal que haya:*

- *k_1 elecciones posibles para el primer termino.*
- *Para cada elección de primer termino, k_2 elecciones posibles para el segundo termino.*
- *Para cada elección de los dos primeros términos, k_3 elecciones posibles para el tercer termino.*
- *...*

Entonces S tiene $k_1 \cdot k_2 \cdot k_2 \cdots k_n$ elementos.

Este principio tiene dos aplicaciones particularmente interesantes, que detallamos a continuación:

- Cuando las elecciones para el primer termino forman un conjunto A_1, las elecciones para el segundo termino forman un conjunto A_2, ... y las elecciones de los diferentes términos son independientes entre si. Entonces S es exactamente el producto cartesiano $A_1 \times A_2 \times \cdots \times A_n$. Es el caso del ejemplo 1.10, con $A_1 = A_2 = A_3 = A_4 = \{a, c, s\}$.
- Para contar las palabras de longitud dada sin repetición sobre un alfabeto A. Es el caso del ejemplo 1.11, con el conjunto de los estudiantes como alfabeto.

El cardinal del producto cartesiano

Aplicando el principio del producto al recuento del producto cartesiano $A_1\times A_2\times\cdots\times A_n$, obtenemos que el cardinal del producto cartesiano es el producto de los cardinales:

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$$

Un caso particular es cuando todos los conjuntos A_i son iguales a un mismo conjunto A. Entonces obtenemos:

$$|A^n| = |A|^n$$

Recordar que este conjunto A^n tiene las interpretaciones siguientes:

- El conjunto de las sucesiones de longitud n con términos en A.
- El conjunto de las palabras de longitud n en el alfabeto A.
- El conjunto de todas las aplicaciones de $\{1, 2, \ldots, n\}$ en A.

Ejemplo 1.12 **Pregunta:** ¿ Cuántos subconjuntos tiene $\{1, 2, 3, \ldots, 10\}$?

Solución: sea S el conjunto de los subconjuntos de $\{1, 2, 3, \ldots, 10\}$ y B el conjunto de las sucesiones de 10 bits. Definimos una biyección de S en B de la manera siguiente: a un subconjunto T de $\{1, 2, 3, \ldots, 10\}$ asociamos la sucesión $a_1 a_2 \cdots a_{10}$ donde $a_i = 1$ si $i \in T$, sino $a_i = 0$. Por ejemplo a $T = \{1, 5, 7, 10\}$ se asocia: 1000101001.

Por el principio de la biyección, tenemos $|S| = |B|$. Ahora B es simplemente $\{0, 1\}^{10}$. Por lo tanto $B = 2^{10} = 1024$. En conclusión, el conjunto $\{1, 2, 3, \ldots, 10\}$ tiene 1024 subconjuntos. ◊

Razonando de manera similar para un conjunto con un número n cualquiera de elementos, obtenemos el resultado siguiente:

Teorema 1.6 *Un conjunto de n elementos tiene exactamente 2^n subconjuntos.*

Ejemplo 1.13 ¿ Cuántas aplicaciones hay de $\{1, 2, 3\}$ en $\{1, 2, 3, 4, 5, 6\}$?

Solución: Estas aplicaciones son simplemente las palabras de longitud 3 en el alfabeto $\{1, 2, 3, 4, 5, 6\}$, por la interpretación como aplicaciones de las sucesiones, dada en el parágrafo 1.3. Por lo tanto hay 6^3 tales aplicaciones. ◊

De manera general, vemos que el número de aplicaciones del conjunto finito X al conjunto finito Y es $|X|^{|Y|}$.

Ejemplo 1.14 En este ejemplo se aplica tanto el principio de adición como el principio del producto.

En cierto sistema informático, una contraseña válida tiene entre 6 y 8 caracteres válidos. El primero tiene que ser un carácter alfabético, los siguientes son alfabéticos o numéricos. Hay 52 caracteres alfabéticos autorizados. Son:

$$A = \{a, b, c, \ldots, z, A, B, C, \ldots, Z\}$$

y 10 caracteres numéricos autorizados:

$$N = \{0, 1, 2, \ldots, 9\}$$

Pregunta: ¿ Cuántas contraseñas válidas hay ?

Solución: Sea k el número de contraseñas válidas, es el número que buscamos. Sea $S = A \cup N$. El conjunto de las contraseñas validas es:

$$(A \times S^5) \cup (A \times S^6) \cup (A \times S^7)$$

Las contraseñas en $A \times S^5$ son las de 6 caracteres (como por ejemplo "Z34pp1"; "Z" está en A y "34pp1" está en S^5), las contraseñas en $A \times S^6$ tienen longitud 7 y las contraseñas

en $A \times S^7$ tienen longitud 8. Como estos tres conjuntos son disjuntos dos a dos, podemos aplicar la regla de la suma;

$$k = |A \times S^5| + |A \times S^6| + |A \times S^7|$$

Luego aplicando la regla del producto obtenemos:

$$k = |A| \cdot |S^5| + |A| \cdot |S^6| + |A| \cdot |S^7|$$

Aplicando la regla de la suma para $S = A \cup N$ (ya que A y N son disjuntos), obtenemos $|S| = |A| + |N| = 52 + 10 = 62$. Finalmente:

$$k = 52 \cdot 62^5 + 52 \cdot 62^6 + 52 \cdot 62^7 \cong 1,8 \cdot 10^{14} \text{ contraseñas posibles.}$$

$\Diamond$

Palabras sin repetición

Aplicamos ahora la regla del producto para contar las palabras sin repetición, como *abc*, *abd*, *cba*, ... pero no *aba* (repetición de *a*).

¿ Cuántas son las palabras sin repetición de longitud n sobre un alfabeto de k elementos ? Tenemos:

- k elecciones posibles para la primera letra,
- Para cada elección posible de primera letra, $k-1$ elecciones posibles para la segunda letra.
- Para cada elección de las dos primeras letras, $k-2$ elecciones posibles de tercera letra.
- ...

Por lo tanto:

Regla 4 *El número de palabras de longitud n, sin repetición de letras, sobre un alfabeto de k elementos es:*

$$k(k-1)(k-2)\cdots(k-n+1)$$

(Observad que es un producto de n términos).

Ejemplo 1.15 ¿Cuántos números de 3 cifras existen sin cifras repetidas? Respuesta: $10 \times 9 \times 8 = 720$, puesto que hay 10 posibles elecciones para el primer dígito, 9 para el segundo y 8 para el tercero. $\Diamond$

Terminología (por si lo encontrais en alguna lectura): Las palabras sin repetición se llaman a veces *variaciones*.

Permutaciones

Una caso particular del recuento anterior es él de las palabras de longitud n sin repetición sobre un alfabeto de n elementos (mismo n). Estas palabras se llaman *permutaciones* del alfabeto.

Ejemplo 1.16 ¿Cuántos números de tres cifras distintas se pueden escribir con los dígitos 1, 3, 5? Respuesta: son las 6 permutaciones de $\{1, 3, 5\}$, a saber:

$$\begin{array}{lll} 135, & 153, & 315, \\ 351, & 513, & 531 \end{array}$$

$\Diamond$

Como caso particular de la formula para contar las palabras sin repetición de longitud dada sobre un alfabeto dado, vemos que el número de permutaciones de un conjunto de n elementos es:

$$n(n-1)(n-2)\cdots 2 \cdot 1$$

Es el producto de los n primeros enteros no–negativos (el *factorial de* n, notada $n!$). Lo enunciamos como una regla a recordar.

Regla 5 *El número de permutaciones de un conjunto de n elementos es $n!$.*

Observación: La factorial de 0 se definie como: $0! = 1$.

Ejemplo 1.17 ¿ Cuántas son las permutaciones (=anagramas) de la palabra CONTAR ? Ya que CONTAR no tiene letra repetida, es un caso particular de recuento de palabras sin repetición: son las 6! permutaciones del conjunto $\{C, O, N, T, A, R\}$. Se llaman también *permutaciones del conjunto* $\{C, O, N, T, A, R\}$. $\Diamond$

Observación: Hemos visto (en el parágrafo 1.3) que las palabras de longitud n sobre A se identifican con las aplicaciones de $\{1, 2, \ldots, n\}$ en A. Bajo esta identificación, las permutaciones de A se corresponden con las *biyecciones* de $\{1, 2, \ldots, n\}$ en A.

2. El principio de división, el recuento de los subconjuntos de k elementos, y los números binómicos

2.1. El principio de división

Ejemplo 2.1 Queremos montar una red local de 8 ordenadores en anillo doble, es decir como en la figura II.1. Los ordenadores, con números de 1 hasta 8, tienen características diferentes. ¿ Cuántas redes diferentes se pueden montar ? Consideramos dos redes como identicas si tienen la misma topología (es decir: si cada ordenador tiene los mismos vecinos en las dos redes). La topología de una red es importante porque determina que ordenadores se comunican más rápidamente entre sí, y el comportamiento de la red en caso de ruptura de cables.

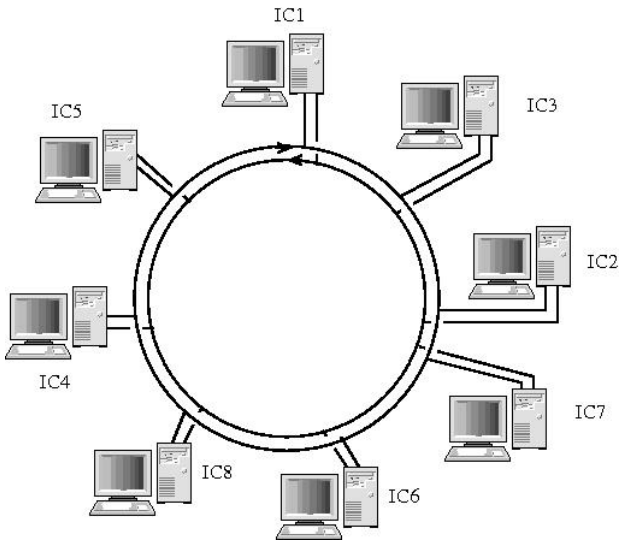


Figura II.1: Ejemplo 2.1.

Intentando reducir el problema a un problema de conteo de sucesiones, podemos introducir la aplicación f que a una permutación de $\{1, 2, \ldots, 8\}$ asocia la configuración donde el ordenador etiquetado con el primer número de la permutación esta en la posición más alta del anillo, el ordenador etiquetado con el segundo número inmediatamente a su derecha ... (por ejemplo la configuración de la figura II.1viene de la permutación 13276845) pero, por cierto, no es una biyección (la configuración de la figura II.1 es la misma que la configuración obtenida de la permutación 23768451 por ejemplo) ... ◊

Vamos a introducir una regla más, para refinar el principio de biyección y resolver problemas como el anterior.

Definición 2.1 Una aplicación $f : A \to B$ es *de grado combinatorio* k si todo elemento del conjunto de llegada B tiene exactamente k antecedentes.

Observación: Las aplicaciones de grado combinatorio 1 son exactamente las aplicaciones biyectivas.

Regla 6 (Principio de división) *Si $f : A \to B$ es de grado combinatorio k entonces $|A| = k \cdot |B|$.*

Ejemplo 2.2 Seguimos con el ejemplo 2.1.

Contamos las permutaciones de $\{1, 2, \ldots, 8\}$ que dan lugar a la misma topología de la red. Son todas las sucesiones de ordenadores que encontramos recorriendo el anillo de una manera u otra. Para una topología de red dada podemos:

- Elegir arbitrariamente un "primer" ordenador en el anillo (8 posibilidades).
- Para cada primer ordenador, podemos elegir uno o el otro sentido para recorrer el anillo (2 posibilidades).

Por el principio del producto, hay 16 permutaciones que corresponden a una topología de red dada.

Aplicando ahora el principio de división, con el conjunto de las permutaciones de $\{1, 2, \ldots, 8\}$ para A, el conjunto de las topologías de red para B, y la aplicación f definida en el ejemplo 2.1, vemos que $|B| = |A|/16 = 8!/16 = 2520$. ◊

Ejemplo 2.3 ¿ Cuántas manos de poker se pueden obtener de un juego de 52 cartas ?

Un mano de poker es cualquier conjunto de 5 cartas. Para contarlas, consideramos en primer lugar las *sucesiones* de 5 cartas, que sabemos contar: son $52 \times 51 \times 50 \times 49 \times 48$ por el principio del producto. Sea S el conjunto de todas las sucesiones (con orden) de 5 cartas extraídas del juego de 52 cartas, y C el conjunto de todos los conjuntos (sin orden) de 5 cartas extraídos del juego. Sea f la aplicación de S en C que olvida el orden. Por ejemplo,

$$f\left((5\clubsuit, 1\heartsuit, K\diamondsuit, Q\diamondsuit, 10\diamondsuit)\right) = f\left((1\heartsuit, 5\clubsuit, K\diamondsuit, Q\diamondsuit, 10\diamondsuit)\right) = \ldots = \{5\clubsuit, 1\heartsuit, K\diamondsuit, Q\diamondsuit, 10\diamondsuit\}$$

Dado un conjunto de 5 cartas, ¿ Cuántos antecedentes tiene por f ? Respuesta: son todas las permutaciones del conjunto, son 5!. Por lo tanto f es de grado combinatorio 5!. Por el principio de división, el cardinal de C es:

$$|C| = \frac{|S|}{5!} = \frac{52 \times 51 \times 50 \times 49 \times 48}{5!} \cong 2,6 \text{ milliones}$$

◊

Lo que hemos hecho en este ejemplo es contar todos los subconjuntos de 5 elementos de un conjunto de 52 elementos.

TERMINOLOGÍA: Los subconjuntos de k elementos de un conjunto dado A se llaman a veces *combinaciones de elementos de A tomados de k en k*. Los números de combinaciones de n elementos tomados de k en k son omnipresentes en matemática, al punto de tener un nombre: *números binómicos*, y un símbolo especial: $\binom{n}{k}$.

Aplicando el principio de división como en el ejemplo 2.3, obtenemos la formula siguiente para los números binómicos:

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+2)(n-k+1)}{k!}$$

Desarrollaremos el estudio de los números binómicos más en detalle en la sección 2.3.

2.2. Permutaciones con repeticiones

Consideramos otra aplicación del principio de división.

Ejemplo 2.4

¿ Cuántos anagramas tiene la palabras "SOSOS" ? ¿ Y "CASCARA" ?

Las mismas preguntas se formulan también así:

¿ Cuántas palabras sobre el alfabeto $\{S, O\}$ tienen 2 ocurrencias de O y tres de S ?
¿ Cuántas palabras sobre el alfabeto $\{C, A, S, R\}$ tienen 2 ocurrencias de C, 3 ocurrencias de A, 1 ocurrencia de S y una ocurrencia de R ?

Ya sabemos contar los anagramas de SOSOS (¿Por que ?) ¿ Como contar los anagramas de CASCARA ? Aplicamos el principio de división. Sea B el conjunto de los anagramas de CASCARA, es el conjunto cuyo cardinal queremos determinar. Introducimos ahora un nuevo alfabeto X, que consiste de copias distintas de sus letras: $X = \{C_1, A_1, S, C_2, A_2, R, A_3\}$. Sea B el conjunto de todas las permutaciones de X. Sea $f : A \to B$ la aplicación que "olvida los índices". Por ejemplo:

$$f(A_1C_1RSA_3C_2A_2) = ACRSACA$$

Entonces f tiene grado combinatorio:

$$3! \times 2! \times 1! \times 1!$$

En efecto, dos permutaciones de X tienen la misma imagen si y sólo si se obtienen cada una de la otra permutando las letras A_1, A_2, A_3 entre ellas y las letras C_1 y C_2 entre ellas (y necesariamente guardando la R y la S fijas)

Por el principio de división:

$$|B| = \frac{|A|}{3!2!1!1!}$$

Pero $|A| = 7!$ (permutaciones de un conjunto de 7 elementos). Por lo tanto:

$$|B| = \frac{7!}{3!2!1!1!} = 420.$$

$\Diamond$

El razonamiento se generaliza, proporcionando el resultado siguiente:

Regla 7 *El número de palabras formadas con exactamente k_1 ocurrencias de un elemento, k_2 ocurrencias de otro elemento, ..., k_r ocurrencias de un elemento distinto de todos los anteriores es:*

$$\frac{n!}{k_1!k_2!\cdots k_r!}$$

donde $n = k_1 + k_2 + \cdots + k_r$ (observsese que es la longitud de la palabra).

2.3. Números binómicos

El número binómico $\binom{n}{r}$ cuenta los subconjuntos de k elementos de un conjunto de n elementos. Damos a continuación unas propiedades útiles e interesantes de estos números.

Proposición 2.2 *Dados dos enteros no–negativos n y k se tiene:*

$$\binom{n}{k} = \binom{n}{n-k} \tag{II.1}$$

Damos dos demostraciones de este resultado.

Demostración. Hemos establecido que:

$$\binom{n}{k} = \frac{n!}{k!(n-k!)}$$

Sustituyendo k por $n-k$ (y, en consecuencia, $n-k$ por $n-(n-k)$, que vale k) en esta formula obtenemos:

$$\binom{n}{n-k} = \frac{n!}{(n-k)!k!}$$

Esto es igual a $\binom{n}{k}$. □

La segunda demostración es una *demostración biyectiva* de la identidad (II.1): consiste en hallar para cada uno de los dos miembros de (II.1) un conjunto que tiene este número de elementos, y luego establecer que estos dos conjuntos están en biyección.

Demostración. Sean X (respectivamente Y) el conjunto de los subconjuntos de cardinal k (resp. $n-k$) de $\{1,2,3,\ldots,n\}$. Entonces $|X| = \binom{n}{k}$ e $|Y| = \binom{n}{n-k}$. Para todo subconjunto A de $\{1,2,3,\ldots,n\}$ a k elementos, notamos $f(A)$ para $\overline{A}$ (el complementario de A). Entonces f es una biyección de X en Y. Por lo tanto, $|X| = |Y|$. Esto establece la identidad (II.1). □

Proposición 2.3 *Para todos enteros n y k con $n \geq 0$ y $k \geq 1$ se tiene:*

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \tag{II.2}$$

Demostración. Definimos los conjuntos siguientes:

- X el conjunto de todos los subconjuntos de $\{1,2,\ldots,n+1\}$.
- A el conjunto de todos los subconjuntos de $\{1,2,\ldots,n+1\}$ que contienen $n+1$.
- B el conjunto de todos los subconjuntos de $\{1,2,\ldots,n+1\}$ que no contienen $n+1$. Ó simplemente, B es el conjunto de todos los subconjuntos de $\{1,2,\ldots,n\}$.

Observamos que $X = A \cup B$, y que esta unión es disjunta. Por lo tanto (por el principio de adición), $|X| = |A| + |B|$. Tenemos $|X| = \binom{n+1}{k}$ y $|B| = \binom{n}{k}$. Para determinar $|A|$, consideramos el conjunto C de todos los subconjuntos de $\{1,2,3,\ldots,n\}$ con $k-1$ elementos. La aplicación $f : C \to A$ definida por $f(S) = S \cup \{n+1\}$ es una biyección. Por lo tanto $|C| = |A|$. Pero $|C| = \binom{n}{k-1}$. Obtenemos así la formula anunciada. □

Calculemos los primeros coeficientes binomiales y los colocamos en la tabla siguiente:

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$
$n=0$	1					
$n=1$	1	1				
$n=2$	1	2	1			
$n=3$	1	3	3	1		
$n=4$	1	4	6	4	1	
$n=5$	1	5	10	10	5	1

Esta tabla se llama *triangulo de Pascal*.

OBSERVACIÓN: Para $n=0$ o $n=k$ se tiene siempre $\binom{n}{k}=1$. Para $k=1$ se tiene $\binom{n}{k}=n$.

Los coeficientes del binomio involucrados en la formula (II.2) están en la configuración siguiente:

$$\begin{matrix}\binom{n}{k-1} & \binom{n}{k} \\ \cdots & \binom{n+1}{k}\end{matrix}$$

La formula (II.2) se interpreta de la manera siguiente con respecto a esta tabla:

> *En la tabla anterior, un coeficiente del binomio es la suma del coeficiente que esta en su norte y del que esta en su noroeste.*

Nos permite por lo tanto calcular los coeficientes binómicos sucesivamente.

Observese sin embargo que esta tabla esta a menudo representada con otras orientaciones, por ejemplo:

$$\begin{array}{ccccccccccc} & & & & 1 & & & & & & \\ & & & 1 & & 1 & & & & & \\ & & 1 & & 2 & & 1 & & & & \\ & 1 & & 3 & & 3 & & 1 & & & \\ 1 & & 4 & & 6 & & 4 & & 1 & & \end{array} \quad \text{o} \quad \begin{array}{cccccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 10 & \cdots & \\ 1 & 4 & 10 & \cdots & & \\ 1 & 5 & \cdots & & & \\ 1 & \vdots & & & & \end{array}$$

Las filas de las tablas anteriores suenan familiares ...

$$\begin{aligned}(x+y)^2 &= x^2+2\,xy+y^2\\ (x+y)^3 &= x^3+3\,x^2y+3\,xy^2+y^3\\ (x+y)^4 &= x^4+4\,x^3y+6\,x^2y^2+4\,xy^3+y^4\\ &\vdots\end{aligned}$$

Proposición 2.4 (Teorema del binomio de Newton) *El número binómico* $\binom{n}{k}$ *es el coeficiente de* $x^k y^{n-k}$ *en el desarrollo de* $(x+y)^n$.

Demostración. Introducimos variables x_1, x_2 ... x_n e y_1, y_2, ..., y_n y consideramos el producto:

$$P_n=(x_1+y_1)(x_2+y_2)\cdots(x_n+y_n)$$

Se obtendrá $(x+y)^n$ sustituyendo x_1, x_2, ... por x e y_1, y_2, ... por y en P_n.

Desarrollamos el producto P_n, por ejemplo:

$$P_3 = x_1x_2x_3 + x_1x_2y_3 + x_1y_2x_3 + y_1x_2x_3 + x_1y_2y_3 + y_1x_2y_3 + y_1y_2x_3 + y_1y_2y_3$$

Cuando desarrollamos P_n tenemos que elegir, en el primer paréntesis, entre x_1 e y_1, en el segundo entre x_2 e y_2, ..., en el último entre x_n e y_n. Por lo tanto en el desarrollo de P_n obtenemos todas las palabras de longitud n en el alfabeto $\{x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n\}$, y cada una está obtenida solamente una vez. Llamamos A a este conjunto de palabras.

Cuando sustituimos x_1, x_2, ... por x e y_1, y_2, ... por y, cada palabra en A esta cambiada en un monomio de la forma $x^p y^{n-p}$. Fijamos k. Sea A_k el conjunto de las palabras en A cambiadas en $x^k y^{n-k}$. Entonces el coeficiente de $x^k y^{n-k}$ en $(x+y)^n$ es $|A_k|$. Sea B_k el conjunto de los subconjuntos de $\{1, 2, \ldots, n\}$ de cardinal k. Entonces A_k esta en biyección con B_k, por la aplicación f que asocia a cada palabra el conjunto de los números que aparecen como índices de los "x" (por ejemplo: $f(x_1y_2x_3) = \{1,3\}$). Por definición de $\binom{n}{k}$, tenemos $|B_k| = \binom{n}{k}$. Por el principio de biyección, $|A_k| = |B_k|$. Así la proposición está demostrada. □

Una forma quizás más simple del teorema del binomio de Newton es la siguiente:

El número binómico $\binom{n}{k}$ es el coeficiente de x^k en el desarrollo de $(1+x)^n$.

Se obtiene de la versión anterior sustituyendo y por 1.

Se puede utilizar esta propiedad como *definición* de los números binómicos. En este caso, tiene sentido considerar $\binom{n}{k}$ con k negativo (vale 0).

ſolo ordine ſitúve mutato, dicentur quæri omnes permutationes rerum illarum.

Res autem permutandæ vel omnes poſſunt eſſe diverſæ, vel aliquot earum eædem; quæ quidem per totidem Alphabeti literas, ſive diverſas ſive eaſdem, commodè deſignabuntur.

1. *Si res omnes permutandæ ſunt diverſæ:*

CUM numerus permutationum in rebus pluribus iniri nequeat, niſi idem priùs in omnibus aliis numero pauciorибus compertus habeatur, liquet in hâc inquiſitione utendum viâ ſyntheticâ, hoc eſt, ordiendum nobis eſſe ab hypotheſibus omnium primis & ſimpliciſſimis:

Unius rei, vel literæ, *a*, una tantùm ſumptio vel poſitio eſt.

Duarum rerum, aut literarum, *a* & *b*, vel *a* præcedit & *b* ſequitur, vel præcedente *b* ſequitur *a*; unde duo ipſarum fiunt ordines *a b* & *b a*.

Tres, porrò, literæ *a*, *b*, *c*, ita collocari poſſunt, ut primus locus vel ipſi *a* vel *b* vel *c* concedatur: ſi *a* primum tenet locum, reliquæ duæ duobus, ut diximus, modis diſponi queunt: ſi *b* in primum locum transferatur, reliquarum duarum duplex itidem poterit eſſe poſitio; quod & intelligendum, ubi tertia *c* primam ſedem occupaverit. Unde trium literarum in univerſum ter duæ, ſeu 6, exiſtunt permutationes *a b c*, *a c b*: *b a c*, *b c a*: *c a b*, *c b a*.

Similitèr, ſi 4 extent literæ *a*, *b*, *c*, *d*, earum unaquæque primum obtinere locum poteſt, intereà dum tres reliquæ, ut nunc oſtenſum, ter bis, ſeu ſexiès, ordinem variabunt: quare cùm earum, quæ primo loco poni poſſunt, ſint quatuor, ſequitur omnes quatuor quater ter bis, ſeu quater ſexies, hoc eſt, vicies quater ſitum inter ſe permutare poſſe.

Ob eandem rationem accedente 5tâ literâ *e* inſtitui poſſunt quinquies tot variationes, quot in caſu præcedenti, hoc eſt, quinquies 24, ſeu 120. Et generalitèr, datis quotcunque literis, numerus permutationum, quas ſubire poſſunt omnes, totiès excedit numerum permutationum, quas recipiunt literæ unâ pauciores, quot ſunt unitates in dato literarum numero. Unde ſponte manat ſequens

3. El principio del palomar y el principio de inclusión–exclusión

3.1. Principio de comparación

La condición que define "función biyectiva" (todo elemento de B es imagen de uno, y sólo un, elemento de A) puede partirse en dos ("uno por lo menos" de un lado, "no más de un" por el otro lado), dando lugar a dos tipos de aplicaciones las aplicaciones *inyectivas* y las aplicaciones *sobreyectivas*.

Definición 3.1 Sea f una función de A en B.

- Decimos que f es *inyectiva* cuando cada elemento del conjunto de llegada B es imagen de, *a lo más*, un elemento del conjunto de partida A.
- Decimos que f es *sobreyectiva* cuando cada elemento del conjunto de llegada B es imagen de *al menos* un elemento del conjunto de partida A.

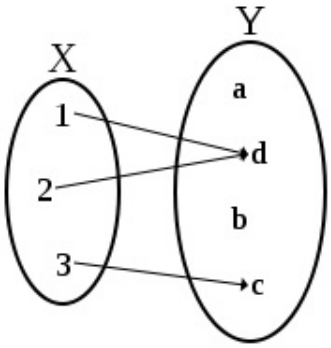
Obsérvese que una aplicación es biyectiva si y sólo si es inyectiva y sobreyectiva a la vez.

Observación: para entender las nociones de "aplicación inyectiva" y "aplicación sobreyectiva", puede ser útil enunciar lo que es para una aplicación $f : A \to B$ *no* ser inyectiva o *no* ser sobreyectiva:

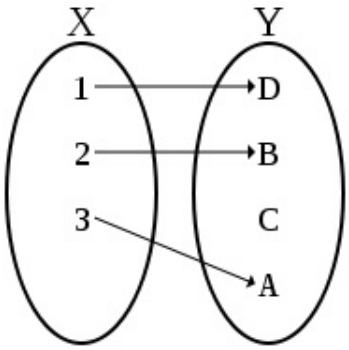
- La aplicación f no es inyectiva si y sólo si existen dos elementos del conjunto de partida A que tienen la misma imagen: $f(a) = f(a')$ con $a \neq a'$.
- La aplicación f no es sobreyectiva si y sólo si existe un elemento del conjunto de llegada B que no sea la imagen de ningún elemento del conjunto de partida A.

Ejemplo 3.1 Hemos visto (parágrafo 1.3) que las aplicaciones con conjunto de partida $\{1, 2, \ldots, n\}$ se identifican con las palabras de longitud n. Vemos que en esta identificación, las aplicaciones *inyectivas* corresponden a las palabras *sin repetición*. ◊

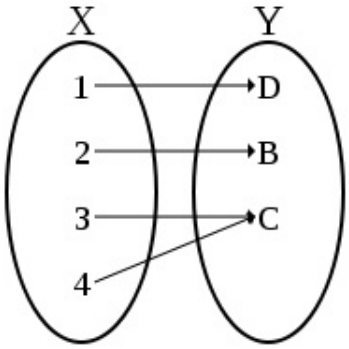
Ejemplo 3.2 El diagrama siguiente representa una función ni inyectiva (d tiene dos antecedantes), ni sobreyectiva (b no tiene antecedante).



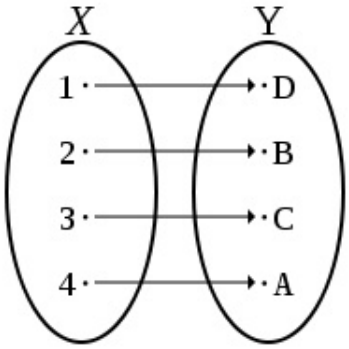
El diagrama siguiente representa una función inyectiva pero no sobreyectiva (C no tiene antecedante):



El diagrama siguiente representa una función sobreyectiva pero no inyectiva (C tiene dos antecedantes):



Este diagrama representa una función a la vez inyectiva y sobreyectiva, es decir: biyectiva.



◊

Regla 8 *Principio de comparación Sea f una aplicación de A en B.*

- *Si f es inyectiva entonces $|A| \leq |B|$.*
- *Si f es sobreyectiva entonces $|A| \geq |B|$.*

3.2. El principio del palomar

Ejemplo 3.3 Si 100 palomas vuelan hacia los 99 nichos de un palomar, entonces por lo menos en uno de los nichos habrá dos o más palomas. ◊

No hace falta seguir la clase de IMD para saber esto ... pero si la misma idea se aplica al problema siguiente, ¿ Suena más interesante ?

Ejemplo 3.4 Considerese los 60 números de 15 cifras siguientes:

887964719632934	853595052833373	353509619982551	830081730551540
558079829715801	307576632323256	959631796100512	280379210953414
287229227755456	614322636818484	477470770159150	964060126349588
185696359139546	574393100402120	358758104182863	843847375041982
704043291794585	164943283221929	932251176700079	842476365687260
129996517563239	241354310206714	107264753201775	430048151603065
918930703766236	933789763806865	262826621816025	764046725256856
203255531597317	965760785214437	247116472139512	155568031850258
196140160830560	598577947802257	800411246266011	246457748356885
117050842616421	737669914029536	740543467620656	271869513523706
471598056079794	701491105472926	921393733200788	668448572075951
895397921831942	748605058193416	372197002112284	926502765039260
793443436342175	627143070588176	191487778595898	172981291280290
812999090787980	815653706272151	807868444440746	959818069149332
809176361839847	279183905034511	580827257466009	237622287732636

Afirmamos que existen dos subconjuntos de este conjunto de números, disjuntos y con la misma suma ... ◊

La idea del ejemplo 3.3 se formaliza de la manera siguiente:

Regla 9 (Principio del palomar) *Si $|A| > |B|$ entonces ninguna función $f : A \to B$ es inyectiva. Es decir, para toda aplicación $f : A \to B$, existen dos elementos distintos del conjunto de partida A con la misma imagen por f.*

Obsérvese que esta regla no es otra cosa que el contrarrecíproco del principio de comparación para funciones inyectivas (parágrafo anterior).

Ejemplo 3.5 Demostramos ahora la afirmación hecha en el ejemplo 3.4.

Cada número de la lista es inferior a 10^{15}, y hay 60 números en la lista. Por lo tanto, la suma de todos les elementos de la lista es inferior a 60×10^{15}. Este número es también, claro, una cota superior para la suma de los elementos de cualquier subconjunto del conjunto de los números de la lista. Consideremos la aplicación f que a cada uno de estos subconjuntos asocia la suma de sus elementos. Toma sus valores en $\{1, 2, \ldots, 60 \times 10^{15}\}$. Tenemos $2^{60} > 60 \times 1015$ (en efecto, $2^{10} = 1024 > 1000$, por lo tanto $2^{60} = (2^{10})^6 > (10^3)^6 = 10^{18}$, y, por otra parte,

$10^{18} > 60 \times 10^{15}$). Por el principio del palomar, existen dos subconjuntos A y B del conjunto de los 60 números con la misma suma. Los conjuntos A y B no son necesariamente disjuntos. Pero los conjuntos $A \setminus B$ y $B \setminus A$ lo son, y también tienen la misma suma. ◊

El principio del palomar admite (entre otras) la siguiente generalización:

Regla 10 (Principio del palomar generalizado) *Si $|A| > k|B|$ entonces para toda aplicación $f : A \to B$, existen $k+1$ elementos de A que tienen la misma imagen por f.*

Ejemplo 3.6 En Sevilla capital hay poco más de 700 000 personas, y ciertamente más de 600 000 personas que no son calvas. Entre ellas, hay por lo menos cuatro personas que tienen *exactamente* el mismo número de cabellos. En efecto, nadie tiene más de 200 000 pelos. Sea A el conjunto de los sevillanos no calvos y $B = \{1, 2, \ldots, 200000\}$. Tenemos $|A| > 600000 > 3 \cdot |B|$. Sea $f : A \to B$ la aplicación que a cada sevillano no calvo asocia su número de pelos. Se aplica el principio del palomar generalizado. ◊

3.3. El principio de inclusión y exclusión

En el parágrafo 1.4 hemos contado los elementos de la unión de conjuntos, cuando son disjuntos dos a dos. Aquí examinamos el caso general, quitando la restricción "disjuntos dos a dos".

Ejemplo 3.7 En la plantilla de un equipo de fútbol, todos los jugadores son españoles o argentinos. Diez son españoles (conjunto E), cinco son argentinos (conjunto A) ¿ Cuántos jugadores son en total ? ¿ 10+5=15 ?

¿ Y que pasa ahora si hay 3 jugadores exactamente que tienen la doble nacionalidad (conjunto $A \cap E$) ? Estos jugadores se habrán contado dos veces en la suma $10+5$. Para que sean contados solamente una vez, tenemos que quitar 3 de la suma. Por lo tanto, el número total de jugadores es 10+5-3. O sea, más generalmente:

$$|A \cup E| = |A| + |E| - |A \cap E|$$

Esta formula se llama *formula de inclusión y exclusión* para el cardinal de la unión de dos conjuntos. ◊

Enunciamos este resultado en general:

RESULTADO: *Sean A y B dos conjuntos. Entonces:*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Demostración. Basta con descomponer $A \cup B$ como unión de subconjuntos disjuntos dos a dos y luego aplicar el principio de la suma. Tenemos:

$$A \cup B = (A \setminus (A \cap B)) \cup (B \setminus (A \cap B)) \cup (A \cap B)$$

y los conjuntos a la derecha son disjuntos dos a dos. Por lo tanto:

$$|A \cup B| = |A \setminus (A \cap B)| + |B \setminus (A \cap B)| + |A \cap B|$$

Tenemos también: $A = (A \cap B) \cup (A \setminus (A \cap B))$ con los conjuntos de la derecha disjuntos. Otra vez por el principio de adición: $|A| = |A \cap B| + |A \setminus (A \cap B)|$. Por lo tanto: $|A \setminus (A \cap B)| = |A| - |A \cap B|$. Similarmente, $|B \setminus (A \cap B)| = |B| - |A \cap B|$. Obtenemos así:

$$|A \cup B| = |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B| = |A| + |B| - |A \cap B|$$

□

En el caso de tres conjuntos hay una formula similar.

RESULTADO: *Sean A, B y C tres conjuntos. Entonces:*

$$\begin{aligned} |A \cup B \cup C| = {} & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C| \end{aligned}$$

Ejemplo 3.8 ¿ Cuántas permutaciones del conjunto $\{0, 1, 2, \ldots, 9\}$ contienen, consecutivamente y en este orden: "4" y luego "2", o "0" y luego "4", o "6" y luego "0" ?

Por ejemplo, 9516243870 no conviene, pero 9516042387 si.

Solución: Sea P_{42} el conjunto de las permutaciones que contienen "42". Sea P_{04} el conjunto de las permutaciones que contienen "04", y P_{60} el conjunto de las permutaciones que contienen "60". Estamos buscando $|P_{42} \cup P_{04} \cup P_{60}|$. Aplicamos la formula de inclusión y exclusión anterior:

$$\begin{aligned} |P_{42} \cup P_{04} \cup P_{60}| = {} & |P_{42}| + |P_{04}| + |P_{60}| \\ & - |P_{42} \cap P_{04}| - |P_{42} \cap P_{60}| - |P_{04} \cap P_{60}| \\ & + |P_{42} \cap P_{04} \cap P_{60}| \end{aligned}$$

Contamos en primer lugar los elementos de P_{42}, de la manera siguiente: en todas las permutaciones que contienen "42"podemos agrupar el 4 y el 2 en un nuevo símbolo $\boxed{42}$. Esto define una biyección f de P_{42} en el conjunto de todas las permutaciones de $\{0, 1, 3, \boxed{42}, 5, 6, 7, 8, 9\}$. Por ejemplo:

$$f((9, 5, 1, 6, 0, 4, 2, 3, 8, 7)) = (9, 5, 1, 6, 0, \boxed{42}, 3, 8, 7)$$

Por lo tanto, P_{42} tiene 9! elementos.

Se procede similarmente con los otros 6 conjuntos: $P_{42} \cap P_{04}$ esta en biyección con las permutaciones de $\{\boxed{042}, 1, 3, 5, 6, 7, 8, 9\}$, $P_{42} \cap P_{60}$ esta en biyección con las permutaciones de $\{1, 3, \boxed{42}, 5, \boxed{60}, 7, 8, 9\}$, ...

Finalmente:

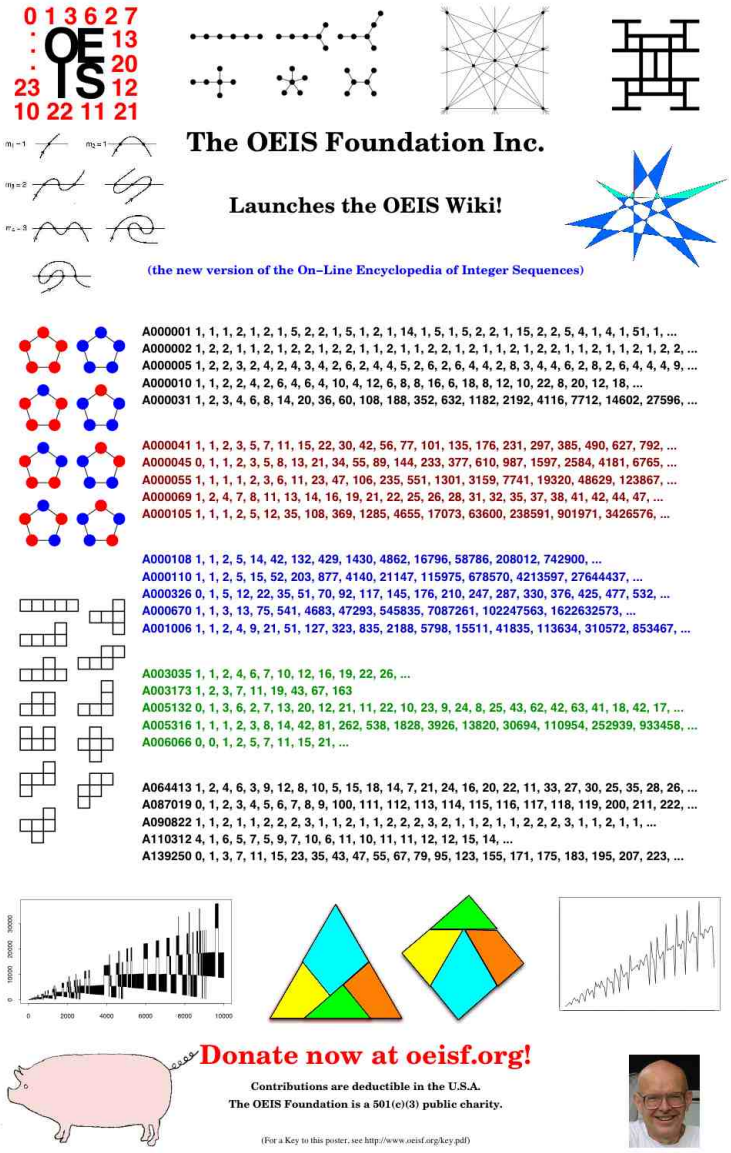
$$\begin{aligned} |P_{42} \cup P_{04} \cup P_{60}| = {} & 9! + 9! + 9! \\ & - 8! - 8! - 8! \\ & + 7! \end{aligned}$$

◊

Enunciamos finalmente la formula en su versión más general.

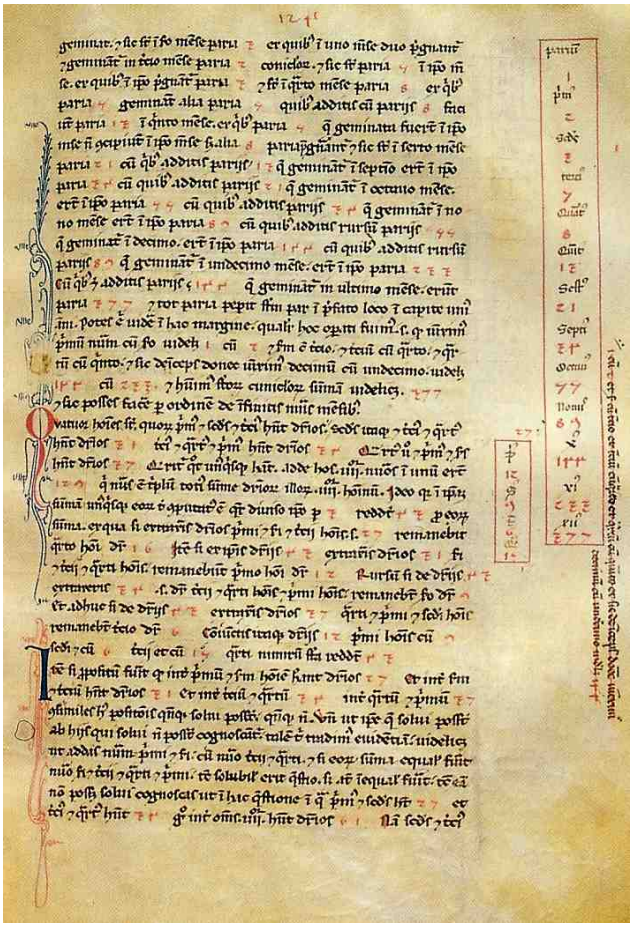
Regla 11 (Principio de inclusión y exclusión) *Sean A_1, A_2, ..., A_n conjuntos. Entonces:*

$$
\begin{aligned}
&|A_1 \cup A_2 \cup \cdots \cup A_n| = \\
&\quad \textit{la suma de los cardinales de los conjuntos} \\
&- \quad \textit{la suma de los cardinales de las intersecciones dos por dos} \\
&+ \quad \textit{la suma de los cardinales de las intersecciones tres por tres} \\
&- \quad \textit{la suma de los cardinales de las intersecciones cuatro por cuatro} \\
&\quad \vdots
\end{aligned}
$$



TEMA III

Recursión



1. Sucesiones

1.1. Introducción

En este tema nos interesamos a *sucesiones de números* infinitas, como las de los ejemplos siguientes:

- la sucesión de los enteros positivos: $(1, 2, 3, 4, 5, 6, \ldots)$
- la sucesión de los cuadrados (de los enteros positivos): $(1, 4, 9, 16, 25, \ldots)$
- la sucesión de los números positivos pares: $(2, 4, 6, 8, 10, \ldots)$
- y la sucesión de los números positivos impares: $(1, 4, 5, 7, 9, \ldots)$
- La sucesión de las potencias de 2: $(1, 2, 4, 8, 16, 32, \ldots)$
- Los ejemplos anteriores son ejemplos de sucesiones de enteros pero podemos considerar también sucesiones de números reales, como las potencias de $\sqrt{2} - 1$:

$$(1, \sqrt{2} - 1, 3 - 2\sqrt{2}, -7 + 5\sqrt{2}, 18 - 12\sqrt{2}, -42 + 30\sqrt{2}, \ldots)$$

- O como las mejores aproximaciones de π con 0, 1, 2, 3, ... cifras después de la coma:

$$(3; 3, 1; 3, 14; 3, 142; 3, 1416; 3, 14159; 3, 141593; 3, 1415927; 3, 14159265; 3, 141592654; \ldots)$$

- Los valores sucesivos de una señal numérica idealizada: figura 1.1.
- Para $n = 1, 2, 3, \ldots$, el número a_n de cadenas de n bits que no tienen ningún par de "0" consecutivos, Para los pequeños valores de n podemos hacer la lista explicita de estas cadenas de bits (cuadro III.1) y contarlas: $a_1 = 2$ para $n = 1$, $a_2 = 3$ para $n = 2$, $a_3 = 5$ para $n = 3$, $a_4 = 8$ para $n = 4$, ...¿ Pero cómo calcular estos números para valores grandes de n ?

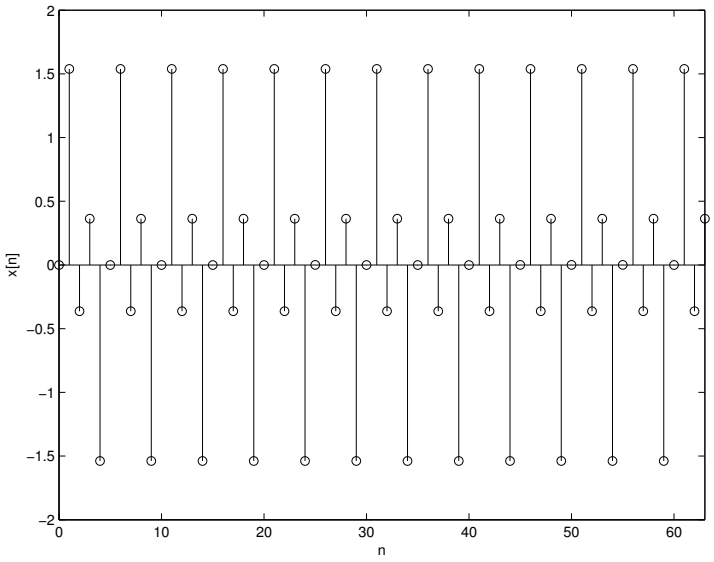
n	valor de a_n	palabras de n bits sin ningún "00"
$n = 1$	$a_1 = 2$	"0", "1"
$n = 2$	$a_2 = 3$	"01", "10", "11"
$n = 3$	$a_3 = 5$	"010", "011", "101", "110", "111"
$n = 4$	$a_4 = 8$	"0101", "0110", "0111", "1010", "1011", "1101", "1110", "1111"
$\vdots$	$a_n =?$	...

Cuadro III.1: Cadenas de n bits sin ningún 00.

1.2. Terminología

Definir una *sucesión numérica* consiste en elegir un intervalo de enteros y asociar un número a cada entero de este intervalo. Por ejemplo, la sucesión de los cuadrados se define asociando a cada entero de $[1, ; +\infty)$ su cuadrado.

Observación: Por lo tanto, una sucesión numérica es simplemente una aplicación (ver Tema II) cuyo conjunto de salida es un intervalo de enteros y cuyo conjunto de llegada es un



$$x[n] = \sin(2\pi f_1 n T_s) + \sin(2\pi f_2 n T_s),\ f_1 = 1\,\text{Hz},\ f_2 = 2\,\text{Hz},\ f_s = 5\,\text{Hz}.$$

Figura III.1: Representación gráfica de una señal numérica periódica (transparencia de una clase de tratamiento de la señal).

conjunto de números ($\mathbb{N}$, $\mathbb{Z}$ o $\mathbb{R}$ en general). Sin embargo, no se emplea para la sucesiones la terminología ni la notación usual de las aplicaciones.

Terminología y notaciones particulares para las sucesiones: Introducimos esta terminología particular considerando la sucesión de los cuadrados. Podemos llamar esta sucesión por ejemplo: c. Entonces:

- 1, 2, 3, 4 ... son los *índices* de la sucesión.
- 1, 4, 9, 16 ... son los *términos* de la sucesión. Se notan también c_1, c_2, c_3, c_4 ...
- Como hay una formula general para los términos c_n (es: $c_n = n^2$), se dice que "c es la sucesión de término general n^2".
- En vez de notar c se puede notar $(c_n)_{n\geq 1}$ (las paréntesis son importantes aquí; el $n \geq 1$ define explícitamente el conjunto de los índices). Se puede también escribir: $c = (n^2)_{n\geq 1}$ ("c es la sucesión de los ene cuadrado, para ene superior o igual a uno").

1.3. Sucesiones definidas recursivamente

Hay varias maneras de definir una sucesión. Consideremos por ejemplo la sucesión de los números positivos pares. La llamamos "u". Tenemos, por lo tanto, $u_1 = 2$, $u_2 = 4$, $u_3 = 6$, ...

- Podemos definirla mediante una formula: $u_n = 2\,n$ para todo n positivo.

- Pero también basta dar su primer valor: $u_1 = 2$, y la regla: "$u_{n+1} = u_n + 2$ para cualquier entero positivo n". En efecto, aplicando la regla para $n = 1$ obtenemos: $u_2 = u_1 + 2 = 2 + 2 = 4$. Luego para $n = 2$: $u_3 = u_2 + 2 = 4 + 2 = 6$. *etc*

Esta segunda descripción de la sucesión se llama *definición recursiva* de la sucesión. Consta de:

- una "condición inicial" ($u_1 = 1$).
- una "relación de recurrencia" que permite calcular cada término a partir de los anteriores ($u_{n+1} = u_n + 2$).

Consideramos otra vez las sucesiones introducidas en 1.1:

- La sucesión de los enteros positivos también es la sucesión $(p_n)_{n\geq 1}$ definida por:

$$\begin{cases} p_1 = 1 & \textit{(condición inicial)} \\ p_{n+1} = p_n + 1 \quad \text{para cualquier } n \geq 1 & \textit{(relación de recurrencia)} \end{cases}$$

- La sucesión $(u_n)_{n\geq 1}$ de los números pares positivos y la sucesión $(v_n)_{n\geq 1}$ de los números impares positivos tienen definiciones recursivas muy parecidas:

$$\begin{cases} u_1 = 2 \\ u_{n+1} = u_n + 2 \quad \text{para cualquier } n \geq 1 \end{cases} \qquad \begin{cases} v_1 = 1 \\ v_{n+1} = v_n + 2 \quad \text{para cualquier } n \geq 1 \end{cases}$$

  Solamente la condición inicial varia.

- La sucesión $(d_n)_{n\geq 0}$ de las potencias de 2 es definida por:

$$\begin{cases} d_0 = 1 \\ d_{n+1} = 2\, d_n \quad \text{para cualquier } n \geq 0 \end{cases}$$

  (similarmente para la sucesión de las potencias de $\sqrt{2} - 1$.)

- La sucesión de las mejores aproximaciones de π no tiene ninguna descripción de este tipo.
- Encontraremos una definición recursiva para la sucesión de los números de cadenas de n bits sin dos "0" consecutivos (ver más abajo el ejemplo 1.2).

Aquí están más ejemplos de sucesiones definidas recursivamente:

- sean α, β, γ tres números. Hay una (única) sucesión $(w_n)_{n\geq 0}$ definida por:

$$\begin{cases} w_0 = \alpha \\ w_{n+1} = \beta\, w_n + \gamma \quad \text{para cualquier } n \geq 0 \end{cases}$$

  Por ejemplo, para $\alpha = 1$, $\beta = 2$, $\gamma = 3$, la definición recursiva de la sucesión es:

$$\begin{cases} w_0 = 1 \\ w_{n+1} = 2\, w_n + 3 \quad \text{para cualquier } n \geq 0 \end{cases}$$

  y sus primeros términos son: 1, 5, 13, 31, 67, ...

- Una relación de recurrencia puede involucrar varios términos anteriores al término definido. Por ejemplo:

$$s_{n+2} = s_{n+1} \times s_n$$

En este caso hace falta varias condiciones iniciales para definir bien la sucesión. Por ejemplo, hay una única sucesión definida por:

$$\begin{cases} s_0 = 2, s_1 = 3 \\ s_{n+2} = s_{n+1} \times s_n \quad \text{para cualquier } n \geq 0 \end{cases}$$

Sus primeros términos son: 2, 3, 6, 18, 108, 1944, ...

- Una definición recursiva puede ser menos explicita. En el método de resolución de ecuaciones por bisección, se considera una función f estrictamente creciente sobre un intervalo $[\alpha;\beta]$, tal que hay una única solución de $f(x) = 0$ en este intervalo. Se hallan aproximaciones de esta solución construyendo dos sucesiones $(a_0, a_1, a_2, a_3, \ldots)$ y $(b_0, b_1, b_2, b_3, \ldots)$ definidas de la manera siguiente:

$$\begin{array}{r} a_0 = \alpha; b_0 = \beta; \text{ y para cualquier } n \geq 0: \\ \text{si } f(\frac{a_n+b_n}{2}) < 0: \quad \begin{cases} a_{n+1} = \frac{a_n+b_n}{2} \\ b_{n+1} = b_n \end{cases} \\ \text{sino:} \quad \begin{cases} a_{n+1} = a_n \\ b_{n+1} = \frac{a_n+b_n}{2} \end{cases} \end{array}$$

1.4. Ecuaciones de recurrencia

Consideramos un ejemplo sencillo pero fundamental.

Ejemplo 1.1 Sea u una sucesión que cumple:

$$u_{n+1} = 2\, u_n \text{ para cualquier } n \geq 0.$$

Entonces calculamos:

$$\begin{aligned} u_1 &= 2\, u_0 \\ u_2 &= 2\, u_1 = 2\, (2\, u_0) = 4\, u_0 \\ u_3 &= 2\, u_2 = 2\, (4\, u_0) = 8\, u_0 \\ &\vdots \end{aligned}$$

No resulta difícil adivinar la formula:

$$u_n = 2^n\, u_0 \text{ para cualquier } n \geq 0.$$

La demostración formal, que no daremos aquí, se hace por inducción. ◊

Una relación de recurrencia, como la del ejemplo 1.1, dónde la sucesión permanece indeterminada, se llama una *ecuación de recurrencia*. *Resolver* esta ecuación, es encontrar todas las sucesiones que la satisfacen. Cada solución es, por lo tanto, una sucesión. En el ejemplo 1.1, hemos resuelto la ecuación de recurrencia:

$$u_{n+1} = 2\, u_n \text{ para cualquier } n \geq 0, \tag{III.1}$$

determinando que sus soluciones son todas las sucesiones de la forma $(t\ 2^n)_{n\geq 0}$ para t número fijo. Por ejemplo, para $t = 1$ tenemos la solución $(2^n)_{n\geq 0}$, cuyos primeros términos

son $(1, 2, 4, 8, 16, \ldots)$. Para $t = 3/2$ tenemos otra solución: la sucesión $(3 \cdot 2^{n-1})_{n\geq 0}$, cuyos primeros términos son $(3/2, 3, 6, 12, 24, \ldots)$.

En dos palabras, hay una formula general para todas las soluciones de la ecuación de recurrencia (esta formula es: $(t\ 2^n)_{n\geq 0}$). En este caso decimos que "$(t\ 2^n)_{n\geq 0}$" es la *solución general* de la ecuación de recurrencia (III.1). Esta solución general depende de un parámetro (el t).

Observación: La "solución general" de una ecuación, cuando depende de parámetros, representa una infinidad de soluciones de la ecuación. Para enfatizar la diferencia entre una *solución* (una sucesión particular que verifica la ecuación) y la *solución general* (una formula general que describe *todas* las soluciones) llamamos a veces "solución particular" lo que es simplemente una solución. Por ejemplo, la solución general de (III.1) es $(t\ 2^n)_{n\geq 0}$, mientras que $(2^n)_{n\geq 0}$ y $(3 \cdot 2^{n-1})_{n\geq 0}$ son dos de sus soluciones particulares.

Analogía importante: Estamos acostumbrados a resolver sistemas de ecuaciones lineales como por ejemplo:

$$\begin{cases} x + y + z &= 0 \\ x - y &= 0 \end{cases} \tag{III.2}$$

Su conjunto de soluciones es el conjunto de los puntos de la forma $(t, t, -2\ t)$ para $t \in \mathbb{R}$. Esta formula $(t, t, -2\ t)$ es la solución general del sistema. Obtenemos las soluciones eligiendo valores para t (el punto $(1, 1, -2)$ para $t = 1$, el punto $(3/2, 3/2, -3)$ para $t = 3/2 \ldots$).

La situación es similar para la ecuación de recurrencia (III.1). Simplemente, en vez de tener 3 variables (x, y, z) tenemos una infinidad (u_0, u_1, u_2 $\ldots$), y en vez de tener dos ecuaciones ($x + y + z = 0$, $x - y = 0$) tenemos una infinidad ($u_1 = 2u_0$, $u_2 = 2u_1$, $u_3 = 2u_2$, $\ldots$).

La pregunta considerada en este tema es la siguiente:

> Dada una ecuación de recurrencia, ¿ Podemos hallar una formula explicita para sus soluciones ?

La respuesta es "no", en general. Vamos a restringir nuestro estudio a una clase importante de ecuaciones de recurrencia, las *ecuaciones de recurrencia lineales a coeficientes constantes*. Para estas sucesiones daremos una receta para hallar formulas explicitas.

Ejemplo 1.2 Si sabemos resolver ecuaciones de recurrencia, nos da herramientas más para determinar formulas para sucesiones en general, aplicando el programa siguiente:

1. Dada una sucesión, buscar una ecuación de recurrencia que satisface.
2. Resolver la ecuación de recurrencia.

Realizamos la fase 1 de este programa para la sucesión $(a_n)_{n\geq 1}$ que cuenta las cadenas de n bits son ningún "00" (último ejemplo en 1.1). La fase 2 (resolución) será realizada en el ejemplo 2.1.

Para una cadena de n bits, $n \geq 3$, sin ningún "00", tenemos la alternativa siguiente:

- o bien termina por 0. En este caso el penúltimo bit tiene que ser 1, y los bits anteriores pueden formar cualquiera cadena de longitud $n - 2$ sin "00".

- o bien termina por "1". En este caso, los bits anteriores pueden formar cualquiera cadena de longitud $n-1$ sin "00".

Hay a_{n-1} cadenas en el primer caso, y a_{n-2} en el segundo. Hemos obtenido que la sucesión de término general a_n verifica:

$$a_n = a_{n-1} + a_{n-2} \text{ para cualquier } n \geq 3$$

o, equivalentemente (poniendo $n = k+2$):

$$a_{k+2} = a_{k+1} + a_k \text{ para cualquier } k \geq 1$$

Tendremos una formula para a_n cuando sabremos resolver este ecuación de recurrencia. ◊

1.5. Ecuaciones de recurrencia lineales

Definicion 1.1 *Una ecuación de recurrencia es lineal a coeficientes constantes cuando es de la forma:*

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} + g(n) \text{ para cualquier } n \geq p$$

dónde k y p son enteros fijos, con $k > 0$, y a_0, a_1, ..., a_{k-1} son números fijos (los coeficientes *de la ecuación), y $g(n)$ es una función de n (el término independiente). El entero k es el* orden de la ecuación. *Si $g(n) = 0$ para cualquier n, entonces se dice que la ecuación de recurrencia es* homogénea.

Ejemplo 1.3 Las ecuaciones siguientes son ecuaciones de recurrencia lineales a coeficientes constantes:

- "$u_{n+1} = 2\, u_n$ para cualquier $n \geq 0$" (de orden 1, homogénea).
- "$u_{n+2} = u_n + 2$ para cualquier $n \geq 1$" (de orden 1, pero no homogénea. Aquí $g(n) = 2$ para cualquier n).
- "$f_{n+2} = f_{n+1} + f_n$ para cualquier $n \geq 0$" (de orden 2, homogénea).
- "$u_{n+1} = u_n + n$ para cualquier $n \geq 0$" (de orden 2, no homogénea. Aquí $g(n) = n$).

La ecuación siguiente no es lineal:

- "$s_{n+2} = s_n s_{n+1}$ para cualquier $n \geq 0$".

La ecuación siguiente es lineal, pero sus coeficientes no son constantes:

- "$u_{n+1} = n u_n$ para cualquier $n \geq 0$". En efecto, el coeficiente de u_n es n, y depende de n.

◊

A continuación examinamos varios ejemplos de ecuaciones de recurrencia lineales a coeficientes constantes y damos, a veces sin demostración ni justificación, su solución general.

2. Resolución de las ecuaciones de recurrencia lineales homogéneas a coeficientes constantes

2.1. La ecuación homogénea de orden 1

Una ecuación de recurrencia lineal homogénea de orden 1 es de la forma:

$$u_{n+1} = au_n \text{ para cualquier } n \geq p \tag{III.3}$$

Es fácil resolverla: tenemos $u_{p+1} = au_p$, $u_{p+2} = au_{p+1} = a(au_p) = a^2u_p$, $u_{p+3} = au_{p+2} = a(a^2u_p) = a^3u_p$, ... Su solución general es $(a^{n-p}u_p)_{n\geq p}$, donde u_p puede ser elegido arbitrariamente y, por lo tanto, tiene el papel de parámetro. Poner $t = u_p/a^p$ permite dar una presentación más simple a la solución general: es $(ta^n)_{n\geq p}$.

Por lo tanto, el conjunto de las soluciones de (III.3) esta formado de la sucesión de las potencias de a y de todos sus múltiples (las sucesiones $(ta^n)_{n\geq 0}$, para todas las elecciones posibles de t en $\mathbb{R}$).

2.2. La ecuación homogénea de orden 2

Una ecuación de recurrencia lineal homogénea de orden 2 es de la forma:

$$u_{n+2} = au_{n+1} + bu_n \text{ para cualquier } n \geq p \tag{III.4}$$

En primer lugar, busquemos las sucesiones de potencias $(\alpha^n)_{n\geq p}$ que cumplen (III.4) (ya que fue fructifero en el caso de las ecuaciones de recurrencia de orden 1). Sea α un número diferente de 0. Entonces $(\alpha^n)_{n\geq p}$ es solución de (III.4) si y solo si:

$$\alpha^{n+2} = a\alpha^{n+1} + b\alpha^n \text{ para cualquier } n \geq p$$

Como $\alpha \neq 0$, podemos simplificar estas ecuaciones, dividiendo ambos lados por α^n. Obtenemos que $(\alpha^n)_{n\geq p}$ es solución de (III.4) si y solo si:

$$\alpha^2 = a\alpha + b \text{ para cualquier } n \geq p$$

Estas ecuaciones, en número infinito, son todas iguales. No es necesario repetirlas. La condición para que $(\alpha^n)_{n\geq p}$ sea solución de (III.4) es meramente:

$$\alpha^2 = a\alpha + b$$

O sea, que α sea solución de la ecuación:

$$x^2 = ax + b$$

Esta ecuación se llama *ecuación característica de la ecuación de recurrencia* (III.4). Al resolver esta ecuación encontramos dos casos:

- En el caso general hay dos raíces distintas. Pueden ser reales, o imaginarias conjugadas ($x + iy$ y $x - iy$ con x e y reales).
- Hay un caso excepcional: cuando el discriminante de la ecuación es 0, hay una única solución, necesariamente real.

Por lo tanto, en el caso general, la ecuación de recurrencia (III.4) admite dos sucesiones de potencias como soluciones. En el caso excepcional admite solamente una.

A partir de estas observaciones pasamos a describir la solución general de (III.4). Lo hacemos sin justificación.

Teorema 2.1 *La solución general de una ecuación de recurrencia lineal homogénea de orden 2 es:*

- $(t_1\alpha^n + t_2\beta^n)_{n\geq p}$, *con* t_1 *y* t_2 *parámetros, cuando la ecuación característica de la ecuación de recurrencia tiene dos soluciones distintas,* α *y* β *siendo estas soluciones.*
- $(P(n)\alpha^n)_{n\geq p}$ *con* $P(n) = t_0 + t_1 n$ *(un polinomio en* n *de grado a lo sumo* 1 *cuyos coeficientes* t_0 *y* t_1 *son parámetros), cuando la ecuación característica tiene una única solución,* α *siendo esta solución.*

Observación: Aquí están dos descripciones de la ecuación característica:

- Es la ecuación que debe verificar α para que la sucesión de potencias $(\alpha^n)_{n\geq p}$ sea solución de la ecuación de recurrencia lineal homogénea.
- Es también la ecuación obtenida de la ecuación de recurrencia lineal homogénea al sustituir u_n, u_{n+1}, u_{n+2} por $x^0(=1)$, x^1, x^2 respectivamente.

Ejemplo 2.1 Vamos a determinar la única sucesión $(a_n)_{n\geq 0}$ que cumple:

$$\begin{cases} a_1 = 2 \\ a_2 = 3 \\ a_{n+2} = a_{n+1} + a_n \text{ para cualquier } n \geq 0. \end{cases}$$

Resolvemos en primer lugar la ecuación de recurrencia:

$$a_{n+2} = a_{n+1} + a_n \text{ para cualquier } n \geq 0.$$

Es lineal homogénea de orden 2. Su ecuación característica es:

$$x^2 = x + 1$$

La resolvemos y obtenemos que tiene dos soluciones:

$$\alpha = \frac{1-\sqrt{5}}{2}, \qquad \beta = \frac{1+\sqrt{5}}{2}$$

Aplicando el teorema 2.1 concluimos que la solución general de la ecuación de recurrencia es: $(t_1\alpha^n + t_2\beta^n)_{n\geq 0}$.

Buscamos ahora la solución particular que cumple $a_1 = 2$ y $a_2 = 3$. Esto consiste en determinar los valores de t_1 y t_2 tal que:

$$\begin{cases} \alpha t_1 & +\beta t_2 & = 2 \\ \alpha^2 t_1 & +\beta^2 t_2 & = 3 \end{cases}$$

Resolviendo este sistema obtenemos como solución única:

$$t_1 = -\frac{2-\beta}{\sqrt{5}}, t_2 = \frac{2-\alpha}{\sqrt{5}}$$

En consecuencia, la única solución del problema es la sucesión de término general:

$$\frac{1}{\sqrt{5}}\left((2-\alpha)\beta^n-(2-\beta)\alpha^n\right)$$

Esta formula no sirve para calcular un término particular a_n (es mejor calcular a_3, a_4, a_5 sucesivamente utilizando la ecuación de recurrencia $a_{n+2}=a_{n+1}+a_n$). Es útil, sin embargo, para estimar asintóticamente a_n. En efecto, $|\beta|>1$ y $|\alpha|<1$. Por lo tanto, para n grande, α^n es despreciable con respecto a β^n y tenemos la estimación:

$$a_n \sim \frac{2-\alpha}{\sqrt{5}}\beta^n$$

$\Diamond$

Ejemplo 2.2 Hallamos la única sucesión que cumple:

$$\begin{cases} u_0 = 0 \\ u_1 = 2 \\ u_{n+2} = 2\,u_{n+1} - u_n \text{ para cualquier } n \geq 0. \end{cases}$$

Resolvemos en primer lugar la ecuación de recurrencia:

$$u_{n+2} = 2\,u_{n+1} - u_n \text{ para cualquier } n \geq 0.$$

Es lineal homogénea de orden 2. Su ecuación característica es $x^2 = 2\,x - 1$, equivalente a $x^2 - 2x + 1 = 0$. Tiene una única solución, $\alpha = 1$. Aplicamos el teorema 2.1. Obtenemos que la solución general de la ecuación de recurrencia es el polinomio de grado 1 cuyos coeficientes son parámetros: $(t_0 + n\,t_1)_{n\geq 0}$ (el factor α^n ya que $\alpha^n = 1^n = 1$).

Buscamos ahora la solución particular que cumple $u_0 = 0, u_1 = 2$. Corresponde a los valores de t_0 y t_1 que verifican:

$$t_0 = 0, t_0 + t_1 = 2.$$

La resolución es inmediata: la única solución del sistema es $t_0 = 0$, $t_1 = 2$. Por lo tanto la única sucesión que verifica las condiciones presentadas es la sucesión de término general $2n$.
$\Diamond$

Ejemplo 2.3 Hallamos la única sucesión que cumple:

$$\begin{cases} v_0 = 1 \\ v_1 = -1 \\ v_{n+2} = 2\,v_{n+1} - 2v_n \text{ para cualquier } n \geq 0. \end{cases}$$

Resolvemos en primer lugar la ecuación de recurrencia:

$$v_{n+2} = 2\,v_{n+1} - 2v_n \text{ para cualquier } n \geq 0.$$

Es lineal homogénea de orden 2. Su ecuación característica es $x^2 = 2\,x - 2$, equivalente a $x^2 - 2x + 2 = 0$. Tiene dos soluciones imaginarias conjugadas: $\alpha = 1 + i$ y $\beta = 1 - i$. Aplicamos el teorema 2.1. Obtenemos que la solución general de la ecuación de recurrencia es la sucesión de término general $t_1(1+i)^n + t_2(1-i)^n$. Para determinar la única solución que cumple $v_0 = 1$, $v_1 = -1$ resolvemos:

$$\begin{cases} t_1 & +t_2 & = 1 \\ (1+i)t_1 & +(1-i)t_2 & = -1 \end{cases}$$

Resolviendo el sistema obtenemos como única solución: $t_1 = 1/2 + i$, $t_2 = 1/2 - i$. Por lo tanto la solución del problema propuesto es la sucesión de término general: $(1/2 + i)(1 + i)^n + (1/2 - i)(1 - i)^n$. ◊

2.3. La ecuación homogénea de orden cualquiera

Sea una ecuación de recurrencia lineal homogénea de orden k a coeficientes constantes:

$$u_{n+k} = a_0 u_n + a_1 u_{n+1} + a_2 u_{n+2} + \cdots + a_{k-1} u_{n+k-1} \text{ para cualquier } n \geq p$$

Formamos su ecuación característica:

$$x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

Recordamos que esta ecuación es:

- la condición que debe cumplir un número $\alpha \neq 0$ para que la sucesión de potencias $(\alpha^n)_{n \geq p}$ sea solución de la ecuación de recurrencia homogénea.
- la expresión obtenida de la ecuación de recurrencia homogénea al sustituir u_{n-1}, u_n, u_{n+1}, u_{n+2} ... por x^{-1}, $x^0 (= 1)$, x^1, x^2 ... respectivamente.

Su grado es el orden de la ecuación (cuando $a_0 \neq 0$).

Tenemos el resultado siguiente:

Teorema 2.2 *Si la ecuación característica de la ecuación homogénea considerada tiene k soluciones distintas (dónde k es el orden de la ecuación), que podemos llamar α_1, α_2, ..., α_k, entonces la solución general de la ecuación homogénea es la sucesión de término general $t_1 \alpha_1^n + t_2 \alpha_2^n + \cdots + t_k \alpha_k^n$.*

Si, al contrario, la ecuación característica tiene menos de k soluciones, α_1, α_2, ..., α_r (con $r < k$) entonces la solución general de la ecuación de recurrencia es la sucesión de término general $P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \cdots + P_r(n)\alpha_r^n$, donde:

- *P_1, P_2, ..., P_r son polinomios cuyos coeficientes son parámetros*
- *y para cualquier i, el grado de P_i es la multiplicidad, menos uno, de α_i como solución de la ecuación característica.*

Ejemplo 2.4 Resolvemos la ecuación de recurrencia:

$$u_{n+4} = -2u_{n+3} + 2u_{n+1} - u_n \text{ para cualquier } n \geq 0.$$

Su ecuación característica es $x^4 = -2x^3 + 2x - 1 = 0$. Es equivalente a: $x^4 + 2x^3 - 2x + 1 = 0$. determinamos, de alguna manera (quizás con la ayuda del ordenador) que $x^4 + 2x^3 - 2x + 1 = (x+1)^3(x-1) = (x-(-1))^3(x-1)$. Por lo tanto, la ecuación característica tiene solamente dos soluciones: 1 (de multiplicidad 3) y -1 (de multiplicidad 1). Aplicando el teorema 2.2, obtenemos como solución general de la ecuación de recurrencia la solución de término general:

$$(t_0 + t_1 n + t_2 n^2)(-1)^n + t_3$$

donde t_0, t_1, t_2, t_3 son parámetros (aquí $t_0 + t_1 n + t_2 n^2$ es el polinomio de grado 2 del teorema, asociado a la solución -1 de multiplicidad 3, y t_0 es el polinomio de grado 0 asociado a la solución 1 de multiplicidad 1). ◊

3. Resolución de ecuaciones de recurrencia lineales no homogéneas a coeficientes constantes

Si consideramos el sistema de ecuaciones lineales:

$$\begin{cases} x+y+z &= 1 \\ x-y &= 2 \end{cases} \tag{III.5}$$

sabemos que su conjunto de soluciones es una recta de $\mathbb{R}^3$, ya que cada una de las dos ecuaciones describe un plano, y que el sistema describe su intersección. Sabemos también que para describir esta recta nos basta determinar un punto cualquiera de la recta (aquí por ejemplo $(3/2, -1/2, 0)$), y un vector director (por ejemplo $(1, 1, -2)$). Este vector director y todos sus múltiples forman el conjunto de las soluciones del sistema homogéneo asociado al sistema (III.5):

$$\begin{cases} x+y+z &= 0 \\ x-y &= 0 \end{cases}$$

La solución general de (III.5) sistema es: $(3/2+t, -1/2+t, -2t) = (3/2, -1, 0)+t(1, 1, -2)$. Observamos, por lo tanto, que es la suma de una solución particular de (III.5) y de la solución general del sistema homogéneo asociado. Esta observación se generaliza a las ecuaciones de recurrencia lineales a coeficientes constantes.

Teorema 3.1 *La solución general de una ecuación de recurrencia lineal a coeficientes constantes es la suma de una solución particular (cualquiera) de la ecuación, y de la solución general de la ecuación homogénea asociada.*

El programa para resolver una ecuación de recurrencia lineal a coeficientes constantes es, por lo tanto:

1. Hallar la solución general de la ecuación homogénea asociada.
2. Hallar una solución particular de la ecuación (completa).
3. Aplicar el teorema 3.1 para concluir.

En consecuencia, para saber resolver las ecuaciones de recurrencia lineales a coeficientes constantes, nos queda solamente a saber como hallar una solución particular de cada ecuación. No hay receta general para esto, por la gran variedad de funciones $g(n)$ posibles para el término independiente. Damos un receta para el caso de los términos $g(n)$ de la forma $Q(n)r^n$, donde r es un número y Q es un polinomio.

Teorema 3.2 *Para una ecuación de recurrencia lineal a coeficientes constantes de la forma:*

$$u_{n+k} = a_0u_n + a_1u_{n+1} + a_2u_{n+2} + \cdots + a_{k-1}u_{n+k-1} + Q(n)r^n \text{ para cualquier } n \geq p$$

donde Q es un polinomio de grado d y r es un número, siempre existe una solución de la forma $T(n)r^n$ con T polinomio de grado superior o igual a d.

Observación: El teorema incluye como casos particulares:

- El caso cuando g es un polinomio (corresponde a $r = 1$).
- El caso cuando g es una función exponencial ($g(n) = r^n$; corresponde a $Q = 1$).

Para hallar esta solución ponemos $u_n = T(n)r^n$, donde T tiene coeficientes indeterminados y grado d. Lo inyectamos en la ecuación de recurrencia y nos da un sistema cuyas incógnitas son los coeficientes de T. Hay dos posibilidades: o bien el sistema admite una solución. Entonces hemos obtenido una solución particular de la ecuación de recurrencia. O bien no admite ninguna solución. Entonces intentamos de nuevo con T de grado $d + 1$ (o superior si falla otra vez). El teorema nos asegura que esta estrategia pagará.

Ejemplo 3.1 Resolvemos la ecuación de recurrencia:

$$u_{n+1} = 2\,u_n + 3 \text{ para cualquier } n \geq 0.$$

Resolvemos en primer lugar la ecuación de recurrencia homogénea asociada. Es inmediato obtener su solución general: es la sucesión de término general $t\,2^n$, donde t es un parámetro. Buscamos ahora una solución particular de la ecuación completa. Como su término independiente es $g(n) = 3$ (un polinomio de grado 0), buscamos una solución particular de la forma $u_n = b$, con b un número fijo (polinomio de grado 0). Sustituyendo u_n y u_{n+1} por b en la ecuación de recurrencia, obtenemos la condición:

$$b = 2\,b + 3 \text{ para cualquier } n \geq 0.$$

Esta condición se simplifica en $b = -3$. Concluimos que la sucesión constante de término general -3 es una solución particular de la ecuación completa. Aplicando el teorema, obtenemos que la solución general de la ecuación de recurrencia es la sucesión de término general $2^n - 3$. ◊

Ejemplo 3.2 Vamos a obtener la solución general de:

$$u_{n+2} = 2\,u_{n+1} - u_n + n^2 \text{ para cualquier } n \geq 0.$$

Hemos obtenido la solución de la ecuación homogénea asociada en el ejemplo 2.2: es la sucesión de término general $t_0 + nt_1$. Como el término independiente de la ecuación completa es un polinomio de grado 2 (este término es n^2), buscamos como solución particular de la ecuación una sucesión dada por un polinomio de grado 2: $u_n = an^2 + bn + c$. Entonces:

$$\begin{aligned} & u_{n+1} = a(n+1)^2 + b(n+1) + c = an^2 + (2a+b)n + (a+b+c) \\ \text{y} \quad & u_{n+2} = a(n+2)^2 + b(n+2) + c = an^2 + (4a+b)n + (4a+2b+c) \end{aligned}$$

Por lo tanto, esta sucesión $(u_n)_{n\geq 0}$ es solución de la ecuación de recurrencia si y solo si:

$$an^2 + (4a+b)n + (4a+2b+c) = 2\left(an^2 + (2a+b)n + (a+b+c)\right) - \left(an^2 + bn + c\right) + n^2$$
$$\text{para cualquier } n \geq 0$$

Identificando los coeficientes de n^2, de n y de n^0 de cada lado obtenemos como condición:

$$\begin{cases} a = 2a - a + 1 \\ (4a+b) = 2(2a+b) - b \\ 4a + 2b + c = 2(a+b+c) - c \end{cases}$$

Este sistema no tiene solución, por culpa de su primera ecuación: $a = 2a - a + 1$, equivalente a $a = a + 1$.

Buscamos, por lo tanto, una solución de la forma $u_n = dn^3 + an^2 + bn + c$. En este caso:

$$\begin{aligned} u_{n+1} &= d(n+1)^3 + a(n+1)^2 + b(n+1) + c \\ &= dn^3 + (a+3d)n^2 + (2a+b+3d)n + (a+b+c+d) \end{aligned}$$

y

$$\begin{aligned} u_{n+2} &= d(n+2)^3 + a(n+2)^2 + b(n+2) + c \\ &= dn^3 + (a+6d)n^2 + (4a+b+12d)n + (4a+2b+c+8d) \end{aligned}$$

Identificando los coeficientes de n^3, de n^2, de n y de n^0 de cada lado obtenemos como condición:

$$\begin{cases} d = 2d - d \\ a + 6d = 2(a+3d) - a + 1 \\ (4a + b + 12d) = 2(2a + b + 3d) - b \\ 4a + 2b + c + 8d = 2(a + b + c + d) - c \end{cases}$$

Este sistema es equivalente a:

$$\begin{cases} 0 = 0 \\ 0 = 1 \\ (4a + b + 12d) = 2(2a + b + 3d) - b \\ 4a + 2b + c + 8d = 2(a + b + c + d) - c \end{cases}$$

Otra vez es incompatible.

Buscamos por lo tanto una solución de la forma: $u_n = en^4 + dn^3 + an^2 + bn + c$. Ahora:

$$\begin{aligned} u_{n+1} &= e(n+1)^4 + d(n+1)^3 + a(n+1)^2 + b(n+1) + c \\ &= en^4 + (d+4e)n^3 + (a+3d+6e)n^2 + (2a+b+3d+4e)n + (a+b+c+d+e) \end{aligned}$$

y

$$\begin{aligned} u_{n+2} &= e(n+2)^4 + d(n+2)^3 + a(n+2)^2 + b(n+2) + c \\ = en^4 + (d+8e)n^3 + (a+6d+24e)n^2 + (4a+b+12d+32e)n + (4a+2b+c+8d+16e) \end{aligned}$$

Nos conduce esta vez al sistema:

$$\begin{cases} e = 2e - e \\ d + 8e = 2(d+4e) - d \\ a + 6d + 24e = 2(a+3d+6e) - a + 1 \\ 4a + b + 12d + 32e = 2(2a+b+3d+4e) - b \\ 4a + 2b + c + 8d + 16e = 2(a+b+c+d+e) - c \end{cases}$$

Es equivalente a:

$$\begin{cases} 0 = 0 \\ 0 = 0 \\ 12e = 1 \\ d + 4e = 0 \\ a + 3d + 7e = 0 \end{cases}$$

Una de sus soluciones es: $a = 5/12$, $b = 0$, $c = 0$, $d = -4/12$, $e = 1/12$. Corresponde a la solución particular de término general $\frac{1}{12}(n^4 - 4n^3 + 5n^2)$ de la ecuación de recurrencia.

Por lo tanto, la solución general de la ecuación de recurrencia es la sucesión de término general:

$$\frac{1}{12}(n^4 - 4n^3 + 5n^2) + t_1 n + t_0$$

con t_0 y t_1 parámetros. ◊

« Quot paria coniculorum in uno anno ex uno pario germinentur.

parium
1
primus
2
Secundus
3
tercius
5
Quartus
8
Quintus
13
Sestus
21
Septimus
34
Octauus
55
Nonus
89
Decimus
144
Undecimus
233
Duodecimus
377

Qvidam posuit unum par cuniculorum in quodam loco, qui erat undique pariete circundatus, ut sciret, quot ex eo paria germinarentur in uno anno : cum natura eorum sit per singulum mensem aliud par germinare ; et in secundo mense ab eorum natiuitate germinant. Quia suprascriptum par in primo mense germinat, duplicabis ipsum, erunt paria duo in uno mense. Ex quibus unum, scilicet primum, in secundo mense geminat ; et sic sunt in secundo mense paria 3 ; ex quibus in uno mense duo pregnantur ; et, gemitiantur in tercio mense paria 2 coniculorum ; et sic sunt paria 5 in ipso mense ; ex quibus in ipso pregnantur paria 3 ; et sunt in quarto mense paria 8 ; ex quibus paria 5 geminant alia paria 5 : quibus additis cum parijs 8, faciunt paria 13 in quinto mense ; ex quibus paria 5, que geminata fuerunt in ipso mense, non concipiunt in ipso mense ; sed alia 8 paria pregnantur ; et sic sunt in sexto mense paria 21 ; cum quibus additis parijs 13, que geminantur in septimo, erunt in ipso paria 34 ; cum quibus additis parijs 21, que geminantur in octauo mense, erunt in ipso paria 55 ; cum quibus additis parijs 34, que geminantur in nono mense, erunt in ipso paria 89 ; cum quibus additis rursum parijs 55, que geminantur in decimo, erunt in ipso paria 144 ; cum quibus additis rursum parijs 89, que geminantur in undecimo mense, erunt in ipso paria 233. Cum quibus etiam additis parijs 144, que geminantur in ultimo mense, erunt paria 377 ; et tot paria peperit suprascriptum par in prefato loco in capite unius anni. Potes enim uidere in hac margine, qualiter hoc operati fuimus, scilicet quod iunximus primum numerum cum secundo, uidelicet 1 cum 2 ; et secundum cum tercio ; et tercium cum quarto ; et quartum cum quinto, et sic deinceps, donec iunximus decimum cum undecimo, uidelicet 144 cum 233; et habuimus suprascriptorum cuniculorum summam, uidelicet 377 ; et sic posses facere per ordinem de infinitis numeris mensibus ».